AGREEMENT

THIS AGREEMENT is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City"), and **ALL AMERICAN RECORDS MANAGEMENT, INC.,** a Colorado corporation, whose address is 15580 E Hinsdale Cir, Centennial, CO 80112 (the "Contractor"), collectively, the "Parties" and individually a "Party."

RECITALS

WHEREAS, the City awarded this Agreement to the Contractor through a competitive selection and the City's Executive Order 8 for the purchase of citywide records management services

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties incorporate the recitals set forth above and agree as follows:

1. **COORDINATION AND LIAISON**: The Contractor shall fully coordinate all services under this Agreement with the City's Chief Information Officer ("CIO") or other designated personnel of the Department of Technology Services ("Agency" or "TS").
2. **SERVICES TO BE PERFORMED**: As the City directs, the Contractor shall diligently undertake, perform, and complete the services and produce all the deliverables set forth in **Exhibit A**, **Scope of Work**, to the City's satisfaction. The Contractor is ready, willing, and able to provide the services required by this Agreement. The Contractor shall faithfully perform the services in accordance with the standards of care, skill, training, diligence, and judgment provided by highly competent individuals performing services of a similar nature to those described in this Agreement and in accordance with the terms of this Agreement.
3. **TERM**: This Agreement will commence on December 1. 2023, and will expire, unless sooner terminated, on December 1, 2028 (the "Term").
4. **COMPENSATION AND PAYMENT**
   - **4.1. Fee**: The City shall pay, and the Contractor shall accept as the sole compensation for services rendered and costs incurred under this Agreement the fees described in the attached exhibits. Amounts billed may not exceed rates set forth in the exhibits and will be made in accordance with any agreed upon payment milestones.
   - **4.2. Reimbursable Expenses**: There are no reimbursable expenses allowed under this Agreement. All of the Contractor's expenses are contained in the exhibits. The City will not be obligated to pay the Contractor for any other fees, costs, expenses, or charges of any nature that may be incurred and paid by the Contractor in performing services under this Agreement including but not limited to personnel, benefits, contract labor, overhead, administrative costs, operating costs, supplies, equipment, and out-of-pocket expenses.
   - **4.3. Invoicing**: The Contractor shall provide the City with a monthly invoice in a format and with a level of detail acceptable to the City including all supporting documentation required by the City. The City's Prompt Payment Ordinance, §§ 20-107 to 20-118, D.R.M.C., applies to invoicing and payment under this Agreement. No term in the exhibits shall modify the City's payment terms and conditions.

4.4. Maximum Contract Amount

4.4.1. Notwithstanding any other provision of this Agreement, the City's maximum payment obligation will not exceed Seven Hundred Fifty Thousand Dollars ($750,000.00) (the "Maximum Contract Amount"). The City is not obligated to execute an Agreement or any amendments for any further services, including any services performed by the Contractor beyond that specifically described in the exhibits. Any services performed beyond those in the exhibits are performed at the Contractor's risk and without authorization under this Agreement.

4.4.2. The City's payment obligation, whether direct or contingent, extends only to funds appropriated annually by the Denver City Council, paid into the Treasury of the City, and encumbered for the purpose of this Agreement. The City does not by this Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. This Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

5. STATUS OF CONTRACTOR: The Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither the Contractor nor any of its employees are employees or officers of the City under Chapter 18 of the Denver Revised Municipal Code, or for any purpose whatsoever.

6. TERMINATION

6.1. The City has the right to terminate this Agreement with cause upon written notice effective immediately, and without cause upon thirty (30) days prior written notice to the Contractor. However, nothing gives the Contractor the right to perform services under this Agreement beyond the time when its services become unsatisfactory to the City.

6.2. Notwithstanding the preceding paragraph, the City may terminate this Agreement if the Contractor or any of its officers or employees are convicted, plead *nolo contendere*, enter into a formal agreement in which they admit guilt, enter a plea of guilty or otherwise admit culpability to criminal offenses of bribery, kickbacks, collusive bidding, bid-rigging, antitrust, fraud, undue influence, theft, racketeering, extortion or any offense of a similar nature in connection with the Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

6.3. The City is entering into this Agreement to serve the public interest. If this Agreement ceases to further the City's public interest, the City, in its sole discretion, may terminate this Agreement, in whole or in part, for convenience by giving written notice to the Contractor.

6.4. Upon termination of this Agreement, with or without cause, the Contractor shall have no claim against the City by reason of, or arising out of, incidental or relating to termination, except for compensation for work duly requested and satisfactorily performed as described in this Agreement.

6.5. If this Agreement is terminated, the City is entitled to and will take possession of all materials, equipment, tools, and facilities it owns that are in the Contractor's possession, custody, or control by whatever method the City deems expedient. The Contractor shall deliver all documents in any

form that were prepared under this Agreement and all other items, materials and documents that have been paid for by the City to the City. These documents and materials are the property of the City. The Contractor shall mark all copies of work product that are incomplete at the time of termination "DRAFT-INCOMPLETE."

7. **EXAMINATION OF RECORDS AND AUDITS**: Any authorized agent of the City, including the City Auditor or his or her representative, has the right to access, and the right to examine, copy and retain copies, at City's election in paper or electronic form, any pertinent books, documents, papers and records related to the Contractor's performance pursuant to this Agreement, provision of any goods or services to the City, and any other transactions related to this Agreement. The Contractor shall cooperate with City representatives and City representatives shall be granted access to the foregoing documents and information during reasonable business hours and until the latter of three (3) years after the final payment under this Agreement or expiration of the applicable statute of limitations. When conducting an audit of this Agreement, the City Auditor shall be subject to government auditing standards issued by the United States Government Accountability Office by the Comptroller General of the United States, including with respect to disclosure of information acquired during the course of an audit. No examination of records and audits pursuant to this paragraph shall require the Contractor to make disclosures in violation of state or federal privacy laws. The Contractor shall at all times comply with D.R.M.C. 20-276.
8. **WHEN RIGHTS AND REMEDIES NOT WAIVED**: In no event will any payment or other action by the City constitute or be construed to be a waiver by the City of any breach of covenant or default that may then exist on the part of the Contractor. No payment, other action, or inaction by the City when any breach or default exists will impair or prejudice any right or remedy available to it with respect to any breach or default. No assent, expressed or implied, to any breach of any term of this Agreement constitutes a waiver of any other breach.
9. **INSURANCE**
   - **9.1. General Conditions**: The Contractor agrees to secure, at or before the time of execution of this Agreement, the following insurance covering all operations, goods or services provided pursuant to this Agreement. The Contractor shall keep the required insurance coverage in force at all times during the term of this Agreement, including any extension thereof, and during any warranty period. The required insurance shall be underwritten by an insurer licensed or authorized to do business in Colorado and rated by A.M. Best Company as "A-VIII" or better. Each policy shall require notification to the City in the event any of the required policies be canceled or non-renewed before the expiration date thereof. Such written notice shall be sent to the parties identified in the Notices section of this Agreement. Such notice shall reference the City contract number listed on the signature page of this Agreement. Said notice shall be sent thirty (30) days prior to such cancellation or non-renewal unless due to non-payment of premiums for which notice shall be sent ten (10) days prior. If such written notice is unavailable from the insurer, the Contractor shall provide written notice of cancellation, non-renewal and any reduction in coverage to the parties identified in the Notices section by certified mail, return receipt requested within three (3) business days of such notice by its insurer(s) and referencing the City's contract

number. The Contractor shall be responsible for the payment of any deductible or self-insured retention. The insurance coverages specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of the Contractor. The Contractor shall maintain, at its own expense, any additional kinds or amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.

9.2. **Proof of Insurance**: The Contractor may not commence services or work relating to this Agreement prior to placement of coverages required under this Agreement. The Contractor certifies that the certificate of insurance attached as **Exhibit B**, preferably an ACORD form, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the certificate of insurance. The City's acceptance of a certificate of insurance or other proof of insurance that does not comply with all insurance requirements set forth in this Agreement shall not act as a waiver of the Contractor's breach of this Agreement or of any of the City's rights or remedies under this Agreement. The City's Risk Management Office may require additional proof of insurance, including but not limited to policies and endorsements.

9.3. **Additional Insureds**: For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), the Contractor and subcontractor's insurer(s) shall include the City and County of Denver, its elected and appointed officials, employees and volunteers as additional insured.

9.4. **Waiver of Subrogation**: For all coverages required under this Agreement, with the exception of Professional Liability—if required, the Contractor's insurer shall waive subrogation rights against the City.

9.5. **Subcontractors and Subconsultants**: The Contractor shall confirm and document that all subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) procure and maintain coverage as approved by the Contractor and appropriate to their respective primary business risks considering the nature and scope of services provided.

9.6. **Workers' Compensation and Employer's Liability Insurance**: The Contractor shall maintain the coverage as required by statute for each work location and shall maintain Employer's Liability insurance with limits of $100,000 per occurrence for each bodily injury claim, $100,000 per occurrence for each bodily injury caused by disease claim, and $500,000 aggregate for all bodily injuries caused by disease claims.

9.7. **Commercial General Liability**: The Contractor shall maintain a Commercial General Liability insurance policy with minimum limits of $1,000,000 for each bodily injury and property damage occurrence, $2,000,000 products and completed operations aggregate (if applicable), and $2,000,000 policy aggregate.

9.8. **Automobile Liability**: The Contractor shall maintain Automobile Liability with minimum limits of $1,000,000 combined single limit applicable to all owned, hired, and non-owned vehicles used in performing services under this Agreement.

9.9. **Professional Liability (Errors & Omissions)**: The Contractor shall maintain minimum limits of $1,000,000 per claim and $1,000,000 policy aggregate limit. The policy shall be kept in force, or a Tail policy placed, for three (3) years for all contracts except construction contracts for which the policy or Tail shall be kept in place for eight (8) years.

9.10. **Commercial Crime**: The Contractor shall maintain minimum limits of $1,000,000 in commercial crime insurance coverage. Coverage shall include theft of City's money, securities, or valuable property by contractor's employees, including any extended definition of employee. The City and County of Denver shall be named as Loss Payee as its interest may appear.

10. DEFENSE AND INDEMNIFICATION

10.1. The Contractor agrees to defend, indemnify, reimburse and hold harmless City, its appointed and elected officials, agents and employees for, from and against all liabilities, claims, judgments, suits or demands for damages to persons or property arising out of, resulting from, or relating to the work performed under this Agreement ("Claims"), unless such Claims have been specifically determined by the trier of fact to be the sole negligence or willful misconduct of the City. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of the Contractor or its subcontractors either passive or active, irrespective of fault, including City's concurrent negligence whether active or passive, except for the sole negligence or willful misconduct of City.

10.2. The Contractor's duty to defend and indemnify City shall arise at the time written notice of the Claim is first provided to City regardless of whether Claimant has filed suit on the Claim. The Contractor's duty to defend and indemnify City shall arise even if City is the only party sued by claimant and/or claimant alleges that City's negligence or willful misconduct was the sole cause of claimant's damages.

10.3. The Contractor shall defend any and all Claims which may be brought or threatened against City and shall pay on behalf of City any expenses incurred by reason of such Claims including, but not limited to, court costs and attorney fees incurred in defending and investigating such Claims or seeking to enforce this indemnity obligation. Such payments on behalf of City will be in addition to any other legal remedies available to City and will not be the City's exclusive remedy.

10.4. Insurance coverage requirements specified in this Agreement in no way lessen or limit the liability of the Contractor under the terms of this indemnification obligation. The Contractor is responsible to obtain, at its own expense, any additional insurance that it deems necessary for the City's protection.

10.5. This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

11. COLORADO GOVERNMENTAL IMMUNITY ACT: In relation to this Agreement, the City is relying upon and has not waived the monetary limitations and all other rights, immunities and protection provided by the Colorado Governmental Act, C.R.S. § 24-10-101, *et seq*.

12. TAXES, CHARGES AND PENALTIES: The City is not liable for the payment of taxes, late charges or penalties of any nature, except for any additional amounts that the City may be required to pay

under the City's prompt payment ordinance D.R.M.C. § 20-107, *et seq*. The Contractor shall promptly pay when due, all taxes, bills, debts and obligations it incurs performing the services under this Agreement and shall not allow any lien, mortgage, judgment or execution to be filed against City property.

13. **ASSIGNMENT; SUBCONTRACTING**: The Contractor shall not voluntarily or involuntarily assign any of its rights or obligations, or subcontract performance obligations, under this Agreement without obtaining the City's prior written consent. Any assignment or subcontracting without such consent will be ineffective and void and will be cause for termination of this Agreement by the City. The City has sole and absolute discretion whether to consent to any assignment or subcontracting, or to terminate this Agreement because of unauthorized assignment or subcontracting. In the event of any subcontracting or unauthorized assignment: (i) the Contractor shall remain responsible to the City; and (ii) no contractual relationship shall be created between the City and any sub-consultant, subcontractor or assign.
14. **INUREMENT**: The rights and obligations of the Parties to this Agreement inure to the benefit of and shall be binding upon the Parties and their respective successors and assigns, provided assignments are consented to in accordance with the terms of this Agreement.
15. **NO THIRD-PARTY BENEFICIARY**: Enforcement of the terms of this Agreement and all rights of action relating to enforcement are strictly reserved to the Parties. Nothing contained in this Agreement gives or allows any claim or right of action to any third person or entity. Any person or entity other than the City or the Contractor receiving services or benefits pursuant to this Agreement is an incidental beneficiary only.
16. **NO AUTHORITY TO BIND CITY TO CONTRACTS**: The Contractor lacks any authority to bind the City on any contractual matters. Final approval of all contractual matters that purport to obligate the City must be executed by the City in accordance with the City's Charter and the Denver Revised Municipal Code.
17. **SEVERABILITY**: Except for the provisions of this Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision of this Agreement or any portion of it to be invalid, illegal, or unenforceable, the validity of the remaining portions or provisions will not be affected, if the intent of the Parties can be fulfilled.
18. **CONFLICT OF INTEREST**: No employee of the City shall have any personal or beneficial interest in the services or property described in this Agreement. The Contractor shall not hire, or contract for services with, any employee or officer of the City that would be in violation of the City's Code of Ethics, D.R.M.C. § 2-51, *et seq*., or the Charter §§ 1.2.8, 1.2.9, and 1.2.12. The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under this Agreement. The Contractor represents that it has disclosed any and all current or potential conflicts of interest. A conflict of interest shall include transactions, activities or conduct that would affect the judgment, actions or work of the Contractor by placing the Contractor's own interests, or the interests of any party with whom the Contractor has a contractual arrangement, in conflict with those of the City. The City, in its sole discretion, will determine the existence of a conflict of interest and may

terminate this Agreement if it determines a conflict exists, after it has given the Contractor written notice describing the conflict.

19. **NOTICES**: All notices required by the terms of this Agreement must be hand delivered, sent by overnight courier service, mailed by certified mail, return receipt requested, electronic mail, or mailed via United States mail, postage prepaid, if to the Contractor at the address above and to City at the addresses below:

    Chief Information Officer, Denver Technology Services
    201 West Colfax Avenue, Dept. 301
    Denver, Colorado 80202

    With a copy to:

    Denver City Attorney's Office
    1437 Bannock St., Room 353
    Denver, Colorado 80202

    Notices hand delivered, sent by electronic mail, or sent by overnight courier are effective upon delivery. Notices sent by certified mail are effective upon receipt. Notices sent by mail are effective upon deposit with the U.S. Postal Service. The Parties may designate substitute addresses where or persons to whom notices are to be mailed or delivered. However, these substitutions will not become effective until actual receipt of written notification.

20. **DISPUTES**: All disputes between the City and the Contractor arising out of or regarding this Agreement will be resolved by administrative hearing pursuant to the procedure established by D.R.M.C. § 56-106(b)-(f). For the purposes of that administrative procedure, the City official rendering a final determination shall be the CIO as defined in this Agreement.

21. **GOVERNING LAW; VENUE**: This Agreement will be construed and enforced in accordance with applicable federal law, the laws of the State of Colorado, and the Charter, Revised Municipal Code, ordinances, regulations and Executive Orders of the City and County of Denver, which are expressly incorporated into this Agreement. Unless otherwise specified, any reference to statutes, laws, regulations, charter or code provisions, ordinances, executive orders, or related memoranda, includes amendments or supplements to same. Venue for any legal action relating to this Agreement will be in the District Court of the State of Colorado, Second Judicial District (Denver District Court).

22. **NO DISCRIMINATION IN EMPLOYMENT**: In connection with the performance of work under this Agreement, the Contractor may not refuse to hire, discharge, promote, demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, ethnicity, citizenship, immigration status, gender, age, sexual orientation, gender identity, gender expression, marital status, source of income, military status, protective hairstyle, or disability. The Contractor shall insert the foregoing provision in all subcontracts.

23. **COMPLIANCE WITH ALL LAWS**: The Contractor shall perform or cause to be performed all services in full compliance with all applicable laws, rules, regulations and codes of the United States, the State of Colorado; and with the Charter, ordinances, rules, regulations and Executive Orders of the

City and County of Denver. These laws, regulations, and executive orders are incorporated by reference herein to the extent that they are applicable to this Agreement and required by law to be so incorporated.

24. **STATUTES, REGULATIONS, AND OTHER AUTHORITY**: Reference to any statute, rule, regulation, policy, executive order, or other authority means such authority as amended, modified, codified, replaced, or reenacted, in whole or in part, and in effect, including rules and regulations promulgated thereunder, and reference to any section or other provision of any authority means that provision of such authority in effect and constituting the substantive amendment, modification, codification, replacement, or reenactment of such section or other provision, in each case except to the extent that this would increase or alter the Parties respective liabilities under this Agreement. It shall be the Contractor's sole responsibility to determine which laws, rules, and regulations apply to the services rendered under this Agreement and to maintain its compliance therewith.
25. **COMPLIANCE WITH DENVER WAGE LAWS**: To the extent applicable to the Contractor's provision of Services hereunder, the Contractor shall comply with, and agrees to be bound by, all requirements, conditions, and City determinations regarding the City's Minimum Wage and Civil Wage Theft Ordinances, Sections 58-1 through 58-26 D.R.M.C., including, but not limited to, the requirement that every covered worker shall be paid all earned wages under applicable state, federal, and city in accordance with the foregoing D.R.M.C. Sections. By executing this Agreement, the Contractor expressly acknowledges that the Contractor is aware of the requirements of the City's Minimum Wage and Civil Wage Theft Ordinances and that any failure by the Contractor, or any other individual or entity acting subject to this Agreement, to strictly comply with the foregoing D.R.M.C. Sections shall result in the penalties and other remedies authorized therein.
26. **LEGAL AUTHORITY**: The Contractor represents and warrants that it possesses the legal authority, pursuant to any proper, appropriate, and official motion, resolution or action passed or taken, to enter into this Agreement. Each person signing and executing this Agreement on behalf of the Contractor represents and warrants that he has been fully authorized by the Contractor to execute this Agreement on behalf of the Contractor and to validly and legally bind the Contractor to all the terms, performances and provisions of this Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend or permanently terminate this Agreement if there is a dispute as to the legal authority of either the Contractor or the person signing this Agreement to enter into this Agreement.
27. **LICENSES, PERMITS, AND OTHER AUTHORIZATIONS**: The Contractor shall secure, prior to the Term, and shall maintain, at its sole expense, all licenses, certifications, permits, and other authorizations required to perform its obligations under this Agreement. This Section is a material part of this Agreement.
28. **PROHIBITED TERMS**: Any term included in this Agreement that requires the City to indemnify or hold the Contractor harmless; requires the City to agree to binding arbitration; limits the Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; or that conflicts with this provision in any way shall be *void ab initio*. Any agreement containing a prohibited term shall otherwise be enforceable as if it did not contain such term or condition, and all agreements

entered into by the City, except for certain intergovernmental agreements, shall be governed by Colorado law notwithstanding any term or condition to the contrary.

29. **DEBARMENT AND SUSPENSION**: The Contractor acknowledges that neither it nor its principals nor any of its subcontractors are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from entering into this Agreement by any federal agency or by any department, agency, or political subdivision of the State of Colorado. The Contractor shall immediately notify the City if any subcontractor becomes debarred or suspended, and shall, at the City's request, take all steps required to terminate its contractual relationship with the subcontractor for work to be performed under this Agreement.
30. **NO CONSTRUCTION AGAINST DRAFTING PARTY**: The Parties and their respective counsel have had the opportunity to review this Agreement, and this Agreement will not be construed against any Party merely because any provisions of this Agreement were prepared by a particular Party.
31. **ORDER OF PRECEDENCE**: In the event of any conflicts between the language of this Agreement and the exhibits, the language of this Agreement controls.
32. **INTELLECTUAL PROPERTY RIGHTS**: The Parties intend that all property rights to any and all materials, text, logos, documents, booklets, manuals, references, guides, brochures, advertisements, URLs, domain names, music, sketches, web pages, plans, drawings, prints, photographs, specifications, software, data, products, ideas, inventions, and any other work or recorded information created by the Contractor and paid for by the City pursuant to this Agreement, in preliminary or final form and on any media whatsoever (collectively, "Materials"), shall belong to the City. The Contractor shall disclose all such items to the City and shall assign such rights over to the City upon completion. To the extent permitted by the U.S. Copyright Act, 17 USC § 101, *et seq*., the Materials are a "work made for hire" and all ownership of copyright in the Materials shall vest in the City at the time the Materials are created. To the extent that the Materials are not a "work made for hire," the Contractor (by this Agreement) sells, assigns and transfers all right, title and interest in and to the Materials to the City, including the right to secure copyright, patent, trademark, and other intellectual property rights throughout the world and to have and to hold such rights in perpetuity. The Parties agree that all materials, text, logos, documents, booklets, manuals, references, guides, brochures, advertisements, URLs, domain names, music, sketches, web pages, plans, drawings, prints, photographs, specifications, software, data, products, ideas, inventions, and any other work or recorded information of the Contractor (collectively, "Contractor Materials") made available, directly or indirectly, by the Contractor to the City as part of the Scope of Services, are the exclusive property of the Contractor or the third parties from whom the Contractor has secured the rights to use such product. Contractor Materials, processes, methods, and services shall remain the property of the Contractor; however, the Contractor hereby grants to the City a nonexclusive, royalty free, perpetual, and irrevocable license to use the Contractor Materials. The Contractor shall mark or identify all such Contractor Materials to the City.
33. **SURVIVAL OF CERTAIN PROVISIONS**: The terms of this Agreement and any exhibits and attachments that by reasonable implication contemplate continued performance, rights, or compliance beyond expiration or termination of this Agreement survive this Agreement and will continue to be

enforceable. Without limiting the generality of this provision, the Contractor's obligations to provide insurance and to indemnify the City will survive for a period equal to any and all relevant statutes of limitation, plus the time necessary to fully resolve any claims, matters, or actions begun within that period.

34. ADVERTISING AND PUBLIC DISCLOSURE: The Contractor shall not include any reference to this Agreement or to services performed pursuant to this Agreement in any of the Contractor's advertising or public relations materials without first obtaining the written approval of the City. Any oral presentation or written materials related to services performed under this Agreement will be limited to services that have been accepted by the City. The Contractor shall notify the City in advance of the date and time of any presentation. Nothing in this provision precludes the transmittal of any information to City officials.

35. CONFIDENTIAL INFORMATION

35.1. "Confidential Information" means all information or data disclosed in written or machine recognizable form and is marked or identified at the time of disclosure as being confidential, proprietary, or its equivalent. Each of the Parties may disclose (a "Disclosing Party") or permit the other Party (the "Receiving Party") access to the Disclosing Party's Confidential Information in accordance with the following terms. Except as specifically permitted in this Agreement or with the prior express written permission of the Disclosing Party, the Receiving Party shall not: (i) disclose, allow access to, transmit, transfer or otherwise make available any Confidential Information of the Disclosing Party to any third party other than its employees, subcontractors, agents and consultants that need to know such information to fulfil the purposes of this Agreement, and in the case of non-employees, with whom it has executed a non-disclosure or other agreement which limits the use, reproduction and disclosure of the Confidential Information on terms that afford at least as much protection to the Confidential Information as the provisions of this Agreement; or (ii) use or reproduce the Confidential Information of the Disclosing Party for any reason other than as reasonably necessary to fulfil the purposes of this Agreement. This Agreement does not transfer ownership of Confidential Information or grant a license thereto. The City will retain all right, title, and interest in its Confidential Information.

35.2. The Contractor shall provide for the security of Confidential Information and information which may not be marked, but constitutes personally identifiable information, HIPAA, CJIS, or other federally or state regulated information ("Regulated Data") in accordance with all applicable laws, rules, policies, publications, and guidelines. If the Contractor receives Regulated Data outside the scope of this Agreement, it shall promptly notify the City.

35.3. Confidential Information that the Receiving Party can establish: (i) was lawfully in the Receiving Party's possession before receipt from the Disclosing Party; or (ii) is or becomes a matter of public knowledge through no fault of the Receiving Party; or (iii) was independently developed or discovered by the Receiving Party; or (iv) was received from a third party that was not under an obligation of confidentiality, shall not be considered Confidential Information under this Agreement. The Receiving Party will inform necessary employees, officials, subcontractors, agents, and officers of the confidentiality obligations under this Agreement, and all requirements

and obligations of the Receiving Party under this Agreement shall survive the expiration or earlier termination of this Agreement.

35.4. Nothing in this Agreement shall in any way limit the ability of the City to comply with any laws or legal process concerning disclosures by public entities. The Parties understand that all materials exchanged under this Agreement, including Confidential Information, may be subject to the Colorado Open Records Act., § 24-72-201, *et seq*., C.R.S., ("CORA"). In the event of a request to the City for disclosure of confidential materials, the City shall advise the Contractor of such request to give the Contractor the opportunity to object to the disclosure of any of its materials which it marked as, or otherwise asserts is, proprietary or confidential. If the Contractor objects to disclosure of any of its material, the Contractor shall identify to the City the legal basis under CORA for any right to withhold. In the event of any action or the filing of a lawsuit to compel disclosure, the Contractor agrees to intervene in such action or lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. If the matter is not resolved, the City will tender all material to the court for judicial determination of the issue of disclosure. The Contractor further agrees to defend, indemnify, and save and hold harmless the City, its officers, agents, and employees, from any claim, damages, expense, loss, or costs arising out of the Contractor's intervention to protect and assert its claim of privilege against disclosure under this Section, including but not limited to, prompt reimbursement to the City of all reasonable attorney fees, costs, and damages that the City may incur directly or may be ordered to pay.

36. PROTECTED INFORMATION AND DATA PROTECTION

36.1. **Compliance with Data Protection Laws**: The Contractor shall comply with all applicable federal, state, local laws, rules, regulations, directives, and policies relating to data protection, use, collection, disclosures, processing, and privacy as they apply to the Contractor under this Agreement, including, without limitation, applicable industry standards or guidelines based on the data's classification relevant to the Contractor's performance hereunder and, when applicable, the most recent iterations of § 24-73-101, *et seq*., C.R.S., IRS Publication 1075, the Health Information Portability and Accountability Act (HIPAA), the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy for all Criminal Justice Information, the Colorado Consumer Protection Act, and the Payment Card Industry Data Security Standard (PCI-DSS), (collectively, "Data Protection Laws"). If the Contractor becomes aware that it cannot reasonably comply with the terms or conditions contained herein due to a conflicting law or policy, the Contractor shall promptly notify the City.

36.2. **Safeguarding Protected Information**: "Protected Information" means data, regardless of form, that has been designated as private, proprietary, protected, or confidential by law, policy, or the City. Protected Information includes, but is not limited to, employment records, protected health information, student records, education records, criminal justice information, personal financial records, research data, trade secrets, classified government information, other regulated data, and personally identifiable information as defined by §§ 24-73-101(4)(b) and 6-1-716(1)(g)(I)(A), C.R.S., as amended. Protected Information shall not include public records that by law must be made available to the public pursuant to the Colorado Open Records Act § 24-72-

201, *et seq*., C.R.S. To the extent there is any uncertainty as to whether data constitutes Protected Information, the data in question shall be treated as Protected Information until a determination is made by the City or an appropriate legal authority. Unless the City provides security protection for the information it discloses to the Contractor, the Contractor shall implement and maintain reasonable security procedures and practices that are both appropriate to the nature of the Protected Information disclosed and that are reasonably designed to help safeguard Protected Information from unauthorized access, use, modification, disclosure, or destruction. Disclosure of Protected Information does not include disclosure to a third party under circumstances where the City retains primary responsibility for implementing and maintaining reasonable security procedures and practices appropriate to the nature of the Protected Information, and the City implements and maintains technical controls reasonably designed to safeguard Protected Information from unauthorized access, modification, disclosure, or destruction or effectively eliminate the third party's ability to access Protected Information, notwithstanding the third party's physical possession of Protected Information. If the Contractor has been contracted to maintain, store, or process personal information on the City's behalf, the Contractor is a "Third-Party Service Provider" as defined by § 24-73-103(1)(i), C.R.S.

36.3. **Data Access and Integrity**: The Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the standards, guidelines, and Data Protection Laws applicable to the Contractor's performance hereunder to ensure the security and confidentiality of all data. The Contractor shall protect against threats or hazards to the security or integrity of data; protect against unauthorized disclosure, access to, or use of any data; restrict access to data as necessary; and ensure the proper use of data. The Contractor shall not engage in "data mining" except as specifically and expressly required by law or authorized in writing by the City. All data and Protected Information shall be maintained and securely transferred in accordance with industry standards. Unless otherwise required by law, the City has exclusive ownership of all data it discloses under this Agreement, and the Contractor shall have no right, title, or interest in data obtained in connection with the services provided herein.

36.4. **Data Retention, Transfer, Litigation Holds, and Destruction**: Using appropriate and reliable storage media, the Contractor shall regularly backup data used in connection with this Agreement and retain such backup copies consistent with the Contractor's data retention policies. Upon termination of this Agreement, the Contractor shall securely delete or securely transfer all data, including Protected Information, to the City in an industry standard format as directed by the City; however, this requirement shall not apply to the extent the Contractor is required by law to retain data, including Protected Information. Upon the City's request, the Contractor shall confirm the data disposed of, the date disposed of, and the method of disposal. With respect to any data in the Contractor's exclusive custody, the City may request that the Contractor preserve such data outside of its usual record retention policies. The City will promptly coordinate with the Contractor regarding the preservation and disposition of any data and records relevant to any current or anticipated litigation, and the Contractor shall continue to preserve the records until

further notice by the City. Unless otherwise required by law or regulation, when paper or electronic documents are no longer needed, the Contractor shall destroy or arrange for the destruction of such documents within its custody or control that contain Protected Information by shredding, erasing, or otherwise modifying the Protected Information in the paper or electronic documents to make it unreadable or indecipherable.

36.5. **Software and Computing Systems**: At its reasonable discretion, the City may prohibit the Contractor from the use of certain software programs, databases, and computing systems with known vulnerabilities to collect, use, process, store, or generate data and information, with Protected Information, received as a result of the Contractor's services under this Agreement. The Contractor shall fully comply with all requirements and conditions, if any, associated with the use of software programs, databases, and computing systems as reasonably directed by the City. The Contractor shall not use funds paid by the City for the acquisition, operation, or maintenance of software in violation of any copyright laws or licensing restrictions. The Contractor shall maintain commercially reasonable network security that, at a minimum, includes network firewalls, intrusion detection/prevention, enhancements, or updates consistent with evolving industry standards, and periodic penetration testing.

36.6. **Background Checks**: The Contractor will ensure that, prior to being granted access to Protected Information, the Contractor's agents, employees, subcontractors, volunteers, or assigns who perform work under this Agreement have all undergone and passed all necessary criminal background screenings, have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Agreement and Data Protection Laws, and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the data.

36.7. **Subcontractors and Employees**: If the Contractor engages a subcontractor under this Agreement, the Contractor shall impose data protection terms that provide at least the same level of data protection as in this Agreement and to the extent appropriate to the nature of the services provided. The Contractor shall monitor the compliance with such obligations and remain responsible for its subcontractor's compliance with the obligations of this Agreement and for any of its subcontractors acts or omissions that cause the Contractor to breach any of its obligations under this Agreement. Unless the Contractor provides its own security protection for the information it discloses to a third party, the Contractor shall require the third party to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the Protected Information disclosed and that are reasonably designed to protect it from unauthorized access, use, modification, disclosure, or destruction. Any term or condition within this Agreement relating to the protection and confidentially of any disclosed data shall apply equally to both the Contractor and any of its subcontractors, agents, assigns, employees, or volunteers. Upon request, the Contractor shall provide the City copies of its record retention, data privacy, and information security policies.

36.8. **Security Breach**: If the Contractor becomes aware of an unauthorized acquisition or disclosure of unencrypted data, in any form, that compromises the security, access,

confidentiality, or integrity of Protected Information or data maintained or provided by the City ("Security Breach"), the Contractor shall notify the City in the most expedient time and without unreasonable delay. The Contractor shall fully cooperate with the City regarding recovery, lawful notices, investigations, remediation, and the necessity to involve law enforcement, as determined by the City and Data Protection Laws. The Contractor shall preserve and provide all information relevant to the Security Breach to the City; provided, however, the Contractor shall not be obligated to disclose confidential business information or trade secrets. The Contractor shall indemnify, defend, and hold harmless the City for any and all claims, including reasonable attorneys' fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from the City in connection with a Security Breach or lawful notices.

36.9. **Request for Additional Protections and Survival**: In addition to the terms contained herein, the City may reasonably request that the Contractor protect the confidentiality of certain Protected Information or other data in specific ways to ensure compliance with Data Protection Laws and any changes thereto. Unless a request for additional protections is mandated by a change in law, the Contractor may reasonably decline the City's request to provide additional protections. If such a request requires the Contractor to take steps beyond those contained herein, the Contractor shall notify the City with the anticipated cost of compliance, and the City may thereafter, in its sole discretion, direct the Contractor to comply with the request at the City's expense; provided, however, that any increase in costs that would increase the Maximum Contract Amount must first be memorialized in a written amendment complying with City procedures. Obligations contained in this Agreement relating to the protection and confidentially of any disclosed data shall survive termination of this Agreement, and the Contractor shall continue to safeguard all data for so long as the data remains confidential or protected and in the Contractor's possession or control.

37. **PROTECTED HEALTH INFORMATION**: The Contractor shall comply with all legislative and regulatory requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); the Health Information Technology for Economic and Clinical Health Act ("HITECH"); 42 CFR Part 2; the privacy standards adopted by the U.S. Department of Health and Human Services, as amended, 45 C.F.R. parts 160 and 164, subparts A and E; and the security standards adopted by the U.S. Department of Health and Human Services, as amended, 45 C.F.R. parts 160, 162 and 164, subpart C (collectively, "HIPAA Rules"). The Contractor shall implement all necessary protective measures to comply with HIPAA Rules, and the Contractor hereby agrees to be bound by the terms of the Business Associate Agreement attached hereto and incorporated herein by reference as **Exhibit G**. The Contractor shall not use protected health information or substance use treatment records except as legally necessary to fulfill the purpose of this Agreement and shall hold the City harmless, to the extent permitted by law, for any breach of these regulations. This Section shall survive the expiration or earlier termination of this Agreement, and the Contractor shall ensure that the requirements of this Section are included in any relevant subcontracts.

38. **CRIMINAL JUSTICE INFORMATION**: Access to and use of criminal history record information and other sensitive information maintained in local, state, and FBI-managed criminal justice

information systems by the Contractor are subject to the terms of this Agreement; 28 C.F.R. Part 20, Criminal Justice Information Systems; 18 U.S.C. § 2721, Prohibition on release and use of certain personal information from State motor vehicle records; Public Law 92-544; the National Crime Prevention and Privacy Compact; the National Crime Information Center ("NCIC") operating manual and polices; the most recent Criminal Justice Information Services Security Policy; and **Exhibit H**, the Federal Bureau of Investigation ("FBI") Criminal Justice Information Services Security Addendum, attached hereto and incorporated herein by reference. Private contractors who perform criminal justice functions and have access to Criminal Justice Information ("CJI") shall meet the same training and certification criteria required of governmental agencies performing a similar function and are subject to audit to the same extent as local agencies. Before receiving access to CJI or Federal Criminal History Record Information ("CHRI"), the Contractor and its individual employees must complete the attached CJIS Security Addendum certification page in **Exhibit H**. The Contractor shall maintain signed CJIS Security Addendum certification pages for its personnel and shall provide copies to the City upon request.

39. **TIME IS OF THE ESSENCE**: The Parties agree that in the performance of the terms, conditions, and requirements of this Agreement, time is of the essence.
40. **PARAGRAPH HEADINGS**: The captions and headings set forth herein are for convenience of reference only and shall not be construed to define or limit the terms and provisions hereof.
41. **CITY EXECUTION OF AGREEMENT**: This Agreement will not be effective or binding on the City until it has been fully executed by all required signatories of the City and County of Denver, and if required by Charter, approved by the City Council.
42. **AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS**: This Agreement is the complete integration of all understandings between the Parties as to the subject matter of this Agreement. No prior, contemporaneous or subsequent addition, deletion, or other modification has any force or effect, unless embodied in this Agreement in writing. No oral representation by any officer or employee of the City at variance with the terms of this Agreement or any written amendment to this Agreement will have any force or effect or bind the City.
43. **USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS**: The Contractor shall cooperate and comply with the provisions of Executive Order 94 and its Attachment A concerning the use, possession or sale of alcohol or drugs. Violation of these provisions or refusal to cooperate with implementation of the policy can result in contract personnel being barred from City facilities and from participating in City operations.
44. **ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS**: The Contractor consents to the use of electronic signatures by the City. This Agreement, and any other documents requiring a signature under this Agreement, may be signed electronically by the City in the manner specified by the City. The Parties agree not to deny the legal effect or enforceability of this Agreement solely because it is in electronic form or because an electronic record was used in its formation. The Parties agree not to object to the admissibility of this Agreement in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the

ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

45. **ATTACHED EXHIBITS INCORPORATED**: The following attached exhibits are hereby incorporated into and made a material part of this Agreement: **Exhibit A**, Scope of Work; **Exhibit B**, Certificate of Insurance; **Exhibit C**, Disaster Recovery; **Exhibit D**, Privacy and Security Policy; **Exhibit E**, NAID Certification; **Exhibit F**, Pricing; **Exhibit G**, HIPAA/HITECH BAA; and **Exhibit H**, CJIS Addendum.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Contract Control Number: TECHS-202369046-00
Contractor Name: ALL AMERICAN RECORDS MANAGEMENT

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of:

SEAL

CITY AND COUNTY OF DENVER:

ATTEST:

By: _____

_____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: _____

REGISTERED AND COUNTERSIGNED:

By: _____

By: _____

Contract Control Number: TECHS-202369046-00
Contractor Name: ALL AMERICAN RECORDS MANAGEMENT

By: DocuSigned by: Grant Eckhardt 5E60E0F368CB444... _____

Name: Grant Eckhardt _____
(please print)

Title: President _____
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

EXHIBIT A

SCOPE OF WORK AND TECHNICAL REQUIREMENTS

A.1 SCOPE OF WORK/REQUIREMENTS:

The vendor shall meet the City's needs for retrieval of City records, offsite records / media storage, and document shredding / destruction. Vendor shall provide secure, professionally managed off-site storage services, as well as timely and accurate retrieval and delivery services. City records are comprised of documents of various media types including, but not limited to, paper, microfiche, microfilm, videotapes, and audiotapes. This contract will be used by multiple City agencies. This section details the scope of work and vendor requirements.

Most City and County of Denver records to be stored will be contained in sealed, standard 1.2 cubic feet boxes. There may be additional needs for boxes to be of various other sizes to accommodate drawings, materials, and larger size documents.

The vendor shall never open the sealed boxes. The vendor shall not allow the City's boxes to be retrieved by, opened, or the records contained therein to be viewed by, anyone except authorized City representatives. The City's Records Manager shall provide the vendor with the names of City representatives, by agency, which are routinely authorized to retrieve, open, and view boxes; and, with the names of agency Records Coordinators and Department Managers who may provide written authorization to additional personnel to retrieve, open, and view boxes on a project-specific basis.

To minimize the risk of potential record loss, the vendor must provide an environmentally sound and secure environment at its facility (ies) and vehicles transporting the records. Additionally, the vendor must have established protocols and procedures for records storage, transportation, inventory, pickup, and delivery. The vendor's staff is expected to be professional, drug and alcohol free, possess a valid driver's license, and have clean driving records and no outstanding arrest warrants.
Capacity for storage of City records must be available, at a minimum, to account for the estimated quantities provided in ***Section A.9 ESTIMATED QUANTITIES***. Additional storage capacity needs by the City may occur throughout the life of contract. The vendor shall provide additional storage capacity at the same rate(s).

The vendor shall provide records storage, delivery, and retrieval services during the City's business hours (Monday through Friday, 8:00 am to 5:00 pm). The vendor shall provide a web portal in addition to a local or toll-free phone number or email address for City end users to make service requests, register complaints, request information, etc. The awarded vendor shall respond to all City requests within a two
(2) hour time frame from the time the incident is initiated. All records must be available for retrieval 24 hours per day, 7 days a week, 365 days per year. Request for Standard, Next Day, and Rush storage and/or retrieval services, by any City department must be provided according to the definitions provided in ***Section A.12: DEFINITIONS***.

DELIVERIES:
Deliveries and pick-ups will be to/from multiple locations throughout the City and County of Denver and Denver International Airport (DEN).

INVOICING:

Invoice payments will be made monthly. The City will pay thirty (30) days in arrears after receipt of invoice, the contract price minus any liquidated damages and/or other damages to the vendor. All invoices shall contain details and a breakdown of each work order/records request between the City and the vendor for ease of reconciliation. All goods and services provided including but not limited to pickups, deliveries, retrievals, new accessions, disposal/destructions, new boxes, etc. must be broken down by each individual transaction placed by the City. The invoice should include a breakdown of total cubic feet of storage, an itemization of each work order to include, but not be limited to number of cartons retrieved/picked up, transportation costs, etc. The vendor shall work with City agencies to address agency specific invoicing requests. Detailed invoices shall be available upon request.

Invoices for services will be sent to the City's Records Manager.

If there is a discrepancy with an invoice which warrants a new invoice to be dispatched, the vendor shall notify the City of the changed invoice and denote on the new invoice that the previous invoice has been superseded.

Invoices shall contain, at a minimum, the following information:

1) City Supplier Contract number
2) Purchase Order Number
3) Line item detail of location and services rendered at that location
4) Total charge
5) Unit price of each charge, extended and totaled
6) Quantity of each charge
7) Invoice number and date
8) Itemized charges, including:
    a. Containers serviced / stored summary
    b. Service date(s) or service period
    c. Service location (Building name and address)
    d. Trip charge(s)
    e. Any additional agreed upon fees
9) Requesting City Agency contact information
    a. Contact's name, phone number, email address, and Agency's Ship to address
10) Additional Documentation: Copies of the following documents may be required with invoice:
    a. Copy of signed pick-up/delivery ticket (received by City from Vendor during transition).

The City will make every effort to notify the vendor within ten (10) days of receipt of invoice of any items questioned. The vendor shall prepare verification data for the amount claimed and provide complete cooperation during such investigation of any areas in the invoices subject to question.

PURCHASE ORDERS:

City Agency(ies) may establish a Request for Encumbrance (RFE) Purchase Order to place multiple orders using the same Purchase Order number and the Vendor will be required to invoice indicating the same Purchase Order number for multiple purchases over the calendar year. City Agency(ies) may also issue a single RFE Purchase Order for a for a specific instance or project that the Vendor will be required to invoice indicating the specific Purchase Order number.

REMOVAL & ADDITION OF PRODUCTS OR SERVICES:
The City reserves the right to add or remove products or services from the contract. When an addition to the contract is required, the vendor will be invited to submit price quotes for these new services/products. If these quotes are comparable with market prices offered for similar services/products, they may be added to the contract.

VENDOR PERFORMANCE:
The City reserves the right to cancel the whole or any part of the contract due to the vendor failing to perform adequately the services required in the contract. In the event of the vendor failing to perform related services within specifications and conditions of the contract, the City shall issue a written notice of deficiency to the vendor. Should the vendor be issued a deficiency notice, the vendor shall be provided a reasonable opportunity to correct the deficiency prior to the City terminating the contract. If vendor cannot cure and the City terminates the contract, vendor shall bare all costs associated with transitioning all City records to another vendor. Failure to maintain satisfactory performance after notice will be sufficient cause for immediate cancellation of the award.

The vendor must perform under all applicable City and State laws. All vendors are expected to become familiar with the ordering agency's rules, policies, and procedures regarding Records Storage. Vendor will be briefed upon award by agency representatives regarding any special security procedures or policies that are agency specific.

The vendor acknowledges and accepts that, in performance of all work under the terms of this agreement, they may have access to proprietary data or confidential information that may be owned or controlled by the City, and that the disclosure of such proprietary data or information may be damaging to the City or third parties. The vendor agrees that all proprietary data or confidential information provided or otherwise disclosed by the City to them shall be held in confidence. The vendor shall exercise the same standard of care to protect such proprietary data and information as a reasonably prudent vendor would to protect its own proprietary or confidential data. Such proprietary data may be in hardcopy, printed, digital or electronic format.

PERSONALLY IDENTIFIABLE INFORMATION (PII):
Except as expressly provided by the terms of this solicitation, the vendor agrees that it shall not disseminate, transmit, license, sublicense, assign, lease, release, publish, post on the internet, transfer, sell, permit access to, distribute, allow interactive rights to, or otherwise make available the proprietary data or confidential information or any part thereof to any other person, party or entity in any form or media for any purpose other than performing its obligations under this agreement. The vendor further acknowledges that by providing this proprietary data of confidential information, the City is not granting them any right or license to use such data except as provided in this agreement. The vendor further agrees not to disclose or distribute to any other party, in whole or in part, the proprietary data or confidential information without written authorization from an authorized City representative.

The vendor will inform its employees and officers of the obligations under this agreement, and all requirements and obligations of the vendor under this agreement shall survive the expiration or earlier termination of this agreement. The vendor shall not disclose proprietary data or confidential information to subcontractors unless such subcontractors are bound by non-disclosure and confidentiality provisions at lease as strict as those contained in this agreement.

A.2 ADDITIONAL SERVICE REQUIREMENTS:

After hours communications capabilities must be provided at storage locations. The vendor must have procedures for notifying the appropriate City end users of any event that will affect the safety or security of their records.

The vendor shall provide a Customer Service area at their storage facility(ies) to allow for authorized City representatives to review City records at no cost to the City. A City representative shall notify the vendor prior to arrival of such records review.

Sometimes it may be necessary for designated City employees to have frequent access to a certain box(s). To minimize the costs in these cases, the City may elect to send that employee(s) directly to the vendor's storage facility(ies) to perform research and retrieve any box(s) as necessary. No City employee will be given access to City records at the vendor's facility(ies) without routine authorization (see above) or written permission from the appropriate City agency Records Coordinator or appropriate department manager. The Records Coordinator or agency head will coordinate all requests for records. The City Records Manager will coordinate requests by City employees to visit facility(ies) and represent all City agencies. There will be a contract administrator representing all City agencies.

The vendor must have the ability to process requests for pickup and retrieval from cloud services via email or other electronic means if required.

At the termination of the contract (including termination before the full-term), the vendor must allow the City to remove all City records at no additional costs. The vendor shall allow the City up to 90 days to complete the relocation.

A.3 VENDOR INVENTORY/TRACKING REQUIREMENTS:

The City maintains its own electronic database to index records by specified storage boxes. The vendor shall have a secure, web-based database, which uses bar-coded or RFID data to track boxes, which will allow City users access via the internet to track/audit inventory, initiate storage/retrieval requests, request or create reports, etc. The City expects to be able to export necessary data to the vendor, and so will not require any data to be keyed in or maintained by the records center except for the vendor's tracking data. The inventory status of City records must be available to view/track via the vendor's electronic inventory system within 24 hours of each transaction. The vendor's tracking system must be capable of documenting date/time of pickup, delivery, and storage location of the City's records so that each record can be identified and located. The vendor's system must have the capability to upload existing data from and to cloud services, Microsoft Excel, or Access databases at no additional charges to the City. The successful vendor shall work with City representatives in developing an on-line inventory acceptable to the City and which will best serve the City's needs. Data from the existing vendor and box numbers shall be imported at no additional charge to the City. For delivery/retrieval orders placed by City users on-line, vendor's system must default standard delivery/retrieval time at a four-hour schedule.

A.3.a **Lost Items:**

Any record not located and delivered in the expected timelines (see Section B.12) will be considered lost.

A.4 VENDOR EMPLOYEE REQUIREMENTS:

Employee drug testing must be performed on an unscheduled basis. Employee selection for those working with the City account must include: an interview process, reference checks, a Colorado Bureau of Investigation criminal/background record check with proof readily available upon request, driving record verification and drug screening (to be performed prior to employment).

A.5 OTHER SUPPLIES:

The vendor shall provide the City, when requested, standardized records center boxes and magnetic/digital media storage containers in the sizes, outside measurement, according to the specifications noted below. Box lids may be separate from box with a minimum height of 2 ¾". Boxes shall be assembly design. Vertical compression strength shall be equal to or in excess of regular 175-test material. The City reserves the right to inspect sample boxes and media storage containers before award of bid to determine responsiveness. The City reserves the right to purchase storage boxes from other vendors.

The majority of records are stored in boxes made of corrugated paper with inside dimensions of 15" x 12" x 10". The construction of the box is normally a triple wall of corrugated board under the handles and double wall throughout the rest of the box. Records already in boxes will remain in the same box. The vendor must also be able to handle magnetic tape and media cases of various sizes and dimensions.

- Standard Letter/Legal (Double-walled Box) 15"x12"x10"
- Letter Transfile 24"x12"x10"
- Legal Transfile 24"x15"x10"
- The vendor shall provide any required forms and/or barcode labels to the City at no additional charge.

A.6 RECORDS DESTRUCTION:

Records shall be destroyed only after their retention period has expired in accordance with records retention schedules approved by the City. The vendor shall provide written notification for records eligible for destruction at the request of the City agency Records Coordinator, City agency head or City Records Manager. Records shall not be destroyed without written concurrence by the appropriate City agency head or the appropriate City agency Records Coordinator.

The method of destruction for confidential records shall be secure shredding whereby the records are completely destroyed and rendered illegible. Secure shredding shall conform to the latest standards of the National Association for Information Destruction, Inc. or similar trade organizations and any regulations affecting the destruction, disposal, and recycling of paper. All documents submitted for destruction will be shredded to no more than 5/16" x 1-1/8". All material shall be combined/mixed with other material and bundled for recycling or further destruction.

Destruction methods for "public" or non-confidential records (normally available to the general public) may include recycling, or a more thorough destruction method. A box shall not be destroyed until the City has confirmed the box's eligibility for destruction and confirmed the box's identity.

The City reserves the right to destroy records itself or to have a third-party destruction company pick up records

from the vendor's storage location(s) to have the records destroyed.

When confidential records (not for public viewing) have been given authorization to be destroyed, the City reserves the right to witness the destruction process. A Certificate of Destruction (COD) shall be completed for all records destroyed using a format approved by the City Records Manager. The COD shall not be completed until after the records are physically destroyed so as to render them illegible. The COD must be its own document, separate from invoices and must contain information of the records that were destroyed, such as the barcode number of a particular box or record. Upon completion, the COD shall be sent to the appropriate City agency upon request and City Records Manager.

A.7 REPORTING REQUIREMENTS:

The successful vendor shall be required to maintain a record of all service requests that are made in conjunction with this award. The vendor shall provide, as requested, to the City's Records Management Coordinator or end using agency, at no additional charges or fees, and not limited to the following (Reports may be requested on a monthly basis):

- Master Inventory (indicating number and description of total records stored, locations of stored records, especially if stored at more than one of the vendor's storage facility(ies). Report totals, where applicable, shall be by number of boxes/tapes stored and total cubic feet. Vendor shall provide electronic backup copy of Master Inventory to City Records Manager at no charge on a semi-annual basis.
- Reports of Files Retrieved
- Any permanent withdrawals of records
- Check-out report including dates of checkout
- Online metrics dashboard
- Reports of Re-files
- Newly stored records for the month being reported
- Reports of records eligible for destruction
- CODs for records that have been destroyed
- Destruction totals including environmental impact
- Total Usage Report for all City using agencies (including all retrieval, storage/service charges).
- For tape and media storage, vendor may be asked to provide monthly rotation schedules as needed.

A.8 RECORD RETRIEVAL:

Retrievals shall be performed upon demand. The vendor will supply documentation for each retrieval, track each

retrieval by box and name of the individual requesting the retrieval. No boxes are to be given to anyone other than a City agency Records Coordinator, City Agency Head or City representative authorized by their respective agency's Record Coordinator or Agency Head.

If the vendor cannot deliver requested boxes to the City by the time periods established in this scope of work, the City reserves the right to use a third-party courier delivery service for box deliveries at no cost to the City. If the City is charged by the third-party courier, the vendor shall reimburse the City. There will be no monthly limit on retrievals per each month.

To view boxes a City employee must provide proper identification stating that they are the designated Records Coordinator or authorized by the appropriate City agency head.

Re-filing of boxes shall be performed on demand.

Good faith efforts must be made to coordinate deliveries and pickups at the same time and only charge for one trip.

The vendor will not apply a "permanent removal charge" or fee associated with a box that is removed and not returned to storage. The City will notify the vendor of its intent to permanently remove a box and the vendor will remove that box from the City's inventory listing at no charge.

A.9 ESTIMATED QUANTITIES:

The amounts of stored boxes listed and yearly spend are the City's best estimate. It is expressly understood and agreed that the contract is to provide storage space and services for the complete actual requirements of the City for the contract period. For informational purposes only, the City has spent approximately $102,000.00 currently in expenses relating to records storage over the previous year of this contract.

ESTIMATED STORAGE TOTALS	
Cubic Feet	**Boxes**
43,269	**29,837**

ACTIVITY	
Box CF Retrieved	5,666
Box CF Retrieved – Rush	15
Box CF Refiled	1022
Computer Record Change	5
Reference Inquiries	3
Box CF Destroyed – Shredding	3,999
Box CF Receiving and Entry	5,180

A.10 SITE VISIT:

Upon request, throughout the life of the contract, authorized representatives from the City may visit the

vendor's facility(ies) to ensure City requirements are met. City Records Management Coordinators must be able to tour the vendor's storage facility(ies) at any time within a 24-hour notice period to verify compliance with the contract.

A.11 STRUCTURE REQUIREMENTS:

The vendor's facility(ies) shall meet the following minimum requirements.

A.11a. **Facility Requirements**

- Access must be restricted to employees, clients, prospects, and necessary vendors. All visitors must be escorted by a vendor employee at all times.
- Facility(ies) must have secured access including, but not limited to, the following:
    - Secured access
    - Professionally monitored burglar and smoke detection systems
    - 24-hour video surveillance
    - Deadbolt locks on doors
- Fire Protection Systems: All facility(ies) (including shipping/receiving and office areas adjacent to storage areas) used by the vendor for storage of the City's records shall have a 24x7x365 fire protection system and be compliant with NFPA 232, the National Fire Protection Association Standard for the Protection of Records. The preferred type of fire control systems is wet-pipe sprinklers with high temperature rated (250° F to 300° F) heads and water flow alarm. The vendor's facility(ies) must be protected by 24-hour alarm and surveillance systems both interior and exterior, which shall be electronically linked to the local police and fire departments or to a bonded security alarm company who will in turn notify local police and/or fire departments of the emergency. Vault storage area shall use inert gas suppression. For supplemental extinguishers there shall be type ABC fire extinguishers placed strategically throughout all storage, office, and receiving/shipping areas. A desired system will also include fire hose cabinets strategically placed throughout the facility(ies), but all hose cabinets shall be plumbed into the sprinkler systems with flow alarms.
- Facilities must meet the National Archives and Records Administration's Facility Standards for Records Storage Facilities.
- The storage area/facility(ies) must be constructed to prevent damage to records during inclement weather (such as hurricanes or flooding). The vendor must have a Disaster Recovery plan and procedures.
- Facility(ies) must provide proper storage environments for all records regardless of format. The facility(ies) must be equipped with climate-controlled storage areas with dust filters. Climate control shall include heating, air conditioning and humidity controls as required to achieve a temperature variation of +/- 15 degrees from established "base" room temperatures to ensure that records do not deteriorate form heat, cold or humidity. Additionally, the vendor's facility(ies) must be equipped with insect control devices or be serviced by a commercial extermination service on a regular basis.
- The vendor shall provide adequate protection for tapes and magnetic media from electromagnetic

fields/disturbances.

- Facility(ies) management must practice strict adherence to municipal, state, and federal building and zoning codes.
- Major electrical installations should be kept separate from storage areas.
- Electrical breaker boxes should be accessible and clearly identified.
- No electrical outlets should be located near magnetic media.
- Temporary alternative power (generators, etc.) need to be prewired and in place in the event of prolonged power failure.
- Uninterruptible power supply (UPS) should be used for any computers that house information the City may need to access.
- Shelving must be of fire retardant, chemically neutral, steel construction. Bottom shelves shall be at least two (2) inches from the floor. Boxes are not to be stacked more than three high.
- Dock loading area must have a secured entry system with video surveillance and not be visible from the street.
- Facility(ies) shall not have windows in any stack areas.
- Facility(ies) shall be located above the local flood plain.
- The storage area must be separate from any offices or work areas.
- No water, steam or other piping shall be present in the hardcopy records storage area other than pipes for the sprinkler system.
- Roofing above stacks must not have any leaks or protection from water damage must be present above stacks.

A.11.b **Vault Requirements:**

- Administrative areas are separated from the vaulting areas.
- Alarm protection for fire detection and suppression; water seepage and flooding; motion and sound detection; magnetic door contact, and improper access code entry.
- Each vault must have a dedicated alarm for heat and fire suppression tied directly to fire stations.
- Each vault must be monitored 24x7 to maintain acceptable temperature (60° - 70° F); and acceptable humidity (35% - 45%).
- The vendor shall use appropriate containers for transport and storage of magnetic media.

A.11.c **Vehicle Requirements:**

- Vehicle cargo area for climate-controlled transport must be environmentally sound with heating, air-conditioning, humidity controls and monitoring.
- Driver(s) must carry mobile devices for communications.
- Vehicle cargo area must be secured during transportation.
- All vehicles must be locked and alarmed at all times while unattended and have a self-alarming security system.
- Storage bay of vehicle must be secured and separate from main cab.
- Vendor owned and operated vehicles only. No employee personal vehicles.
- Vehicle inspection and maintenance logs shall be retained and available to the City upon request.

A.12 DEFINITIONS:

Standard Delivery: Delivery charge/transportation within the Metro Denver Area or Denver International Airport: Call or order online by 4:30 p.m. – delivery by next business day by 1:00 p.m.; Call or order online by 11:00 a.m. – delivery by 4:30 p.m.

Next Day Delivery: Delivery charge/transportation within the Metro Denver Area or Denver International Airport: Call or order online by 4:30 p.m. – delivery by second business day by 1:00 p.m.; Call or order online by 11:00 a.m. – delivery next business day by 4:30 p.m.

Re-Filing: Records to be returned to off-site storage facility.

New Accessions: First time filing of boxes, microfilm, magnetic and digital media, etc.

A.13 F.O.B. POINT:

All prices quoted must be quoted at a firm price F.O.B. Denver, Colorado, delivered to various locations throughout the City and County of Denver. (see Attachment A – Service Locations) Additional sites may be added or deleted throughout the term of the contract.

A.14 DELIVERY/SERVICE CONSIDERATIONS:

Services shall be rendered as follows for pick-up and/or delivery within the Metro Denver area or at Denver International Airport (DEN):

1) Next Day Pick-up/Delivery: Call or order online by 12:00 pm on Business Day 1, pick-up and/or delivery expected by 12:00 pm on Business Day 2; call or order online by 4:30 pm on Business Day 1, pick-up and/or delivery expected by 4:30 pm on Business Day 2

2) Same Day Pick-up/Delivery: Call or order online by 12:00 pm, pick-up and/or delivery expected by 4:30 pm

3) Rush and After-Hours Pick-up/Delivery: Call or order only at any time, twenty-four (24) hours a day, three hundred sixty-five (365) days a year, pick-up and/or delivery expected within two (2) hours

A.15 SHREDDING DELIVERY AND COLLECTION CONSIDERATIONS:

Prior to the start of service, the vendor shall develop a pick-up schedule for each delivery/collection point with the City Records Manager, and the City Agency site/point of contact. The pick-up schedule shall include, but not be limited to, the start date, event items including special pick-ups, frequency of pick-ups, number of receptacles per delivery/collection point, and all normal hours of service and off-hours of service.

Included in the development of the pick-up schedule, the vendor, City Records Manager, and the City Agency site/point of contact may also develop a site map and/or checklist to ensure that all vendor bins are serviced during the delivery/collection scheduled services. A site map and/or checklist will include where the collection bins are placed within a location. Any updates to a site map and/or checklist will be approved by either the City Records Manager or the City Agency site/point of contact. The City does not assume responsibility for any lost, stolen, or damaged vendor-owned bins while in the possession of the City.

After the first ninety (90) days of service, the City Records Manager and the vendor will review each delivery/collection point in order to adjust the pick-up schedules, if deemed necessary by the City. The review process will continue during the entire duration of the contract on a quarterly or as needed basis.
Prior to each review with the vendor, the City Records Manager will confer with each City Agency site/point of contact to ensure that all information is current and accurate. Also prior to the start of service, the vendor will create the implementation schedule with the City Records Manager, in order to assist with the potential transition.

A.16 BACKGROUND CHECKS AND DISQUALIFICATION

Because of the nature of the scope and requirements herein for the City, the vendor, at their expense, must conduct, or have previously conducted a background check for each of its employees, as well as for the employees of its subcontractors, who will provide services to the City. Background checks are to be conducted through an independent background check third-party and must include the following:

- Social Security Number Trace;
- Federal Criminal Records (includes wants, warrants, arrests, convictions, and incarcerations);
- Colorado Criminal Records (includes wants, warrants, arrests, convictions, and incarcerations);
- Criminal Records from other States if the employee disclosed, or the background check identifies, that the employee lived in another state in the last seven years (includes wants, warrants, arrests, convictions, and incarcerations); and
- National Sexual Offender Registry Search.

The background check shall include all convictions for the last seven years and may include additional convictions beyond seven years when permitted and/or required by law.

Because of the sensitive nature of the work, the City shall automatically disqualify from employment under this contract persons with felony convictions. Alternatively, the City may require that a fidelity bond, or such other assurance in such amount as deemed appropriate, be provided to the City as a condition precedent to grant permission where an employee's prior conviction would otherwise preclude their participation under the contract.

All Contractor employees are required to self-disclose to the Contractor any criminal charges and convictions and nolo contendere pleas (not contest pleas) that occur while providing services to the City within three business days of the conviction, charge, or plea. Contractor is required to inform the City of any criminal charges or convictions or nolo contendere pleas (no contest pleas) that arise while an employee is on assignment with the City. Contractor must inform the City within one business day of the Contractor having knowledge of the charge, conviction, or plea. The City will determine, in its sole discretion, whether the employee will remain on a City assignment.

Contracts for work at the following locations require NCIC background checks:

- Police Academy
- Denver Animal Shelter
- Traffic Operations
- DPD Police Precincts
- DPD Crime Lab
- Medical Examiner

Other City locations may also require a NCIC background check. These background checks will be administered by the City and will be at no cost to the Contractor. Contractor employees will be required to provide their social security numbers to the City. Contractors will be provided entrance cards for each facility. Contractors are not allowed to share cards to provide services. The background check(s) must be conducted successfully prior to initial access and/or involvement by employees. Employees who separate from the Contractor's employment must undergo another background check prior to renewed access and/or involvement in providing services to the City. The City also has the ability to audit the Contractor's background check process, to ensure compliance with City standards, at any time. Additionally, failure by the Contractor to comply with the terms of this Section may result in the termination of its contract with the City.

All work to be completed under this Contract will require that each person working on-site at a Denver Police Facility, City Attorney, Denver 911, Denver DA, and all other secure facilities within the City and County of Denver that has CJIS information, including all sub-contractors, to have completed CJIS Security Awareness Training. The CJIS Security Policy written and maintained by the Federal Bureau of Investigation is the standard by which all criminal justice agencies nationwide must protect the sensitive data they possess and share with authorized entities.

The policy outlines requirements such as personnel security, training, encryption, physical security, media protection, access control, construction, and more.

The CBI CJIS Vendor Management Program is designed to help vendors and criminal justice agencies achieve and maintain compliance more easily by providing an easier fingerprinting/vetting process, assisting with the required training, sharing audit findings, and offering resources for questions about CJIS security.

There are two options for completing this process prior to starting any work:

CJIS Access Vendor Program – Through Colorado Bureau of Investigation (CBI)

This option is to complete the process through the Colorado Bureau of Investigation (CBI) vendor program. Vendors can review the requirements at https://cbi.colorado.gov/sections/cjis-security/cjis-vendor-management-program/cjis-access-vendors. There is a fee of $39.50 per individual (as of 1/1/2022), but it takes the least time to complete. Vendors shall follow the steps outlined on the website. This process allows individuals to complete the fingerprinting at any number of locations throughout the metro area.

This is the preferred option and is required when there are more than two (2) employees (including subcontractors) requiring CJIS Training.

A.17 AIRPORT SECURITY:

It is a material requirement of this Contract that the Vendor shall comply with all rules, regulations, written policies, and authorized directives from the City and/or the Transportation Security Administration with respect to Airport security. The Vendor shall conduct all of its activities at the Airport in compliance with the Airport security program, which is administered by the Security Section of the Airport Operations Division, Department of Aviation. Violation by the Vendor or any of its employees, subcontractors, and vendors of any rule, regulation, or authorized directive from the City or the Transportation Security Administration with respect to Airport Security shall be grounds for immediate termination by the City of this Contract for cause.

The Vendor shall promptly upon notice of award of this Contract, meet with the Airport's Assistant Security Manager to establish badging and vehicle permit requirements for Vendor's operations under this Contract. The Vendor shall obtain the proper access authorizations for all of its employees, subcontractors, and vendors who will enter the Airport to perform work or make deliveries and shall be responsible for each such person's compliance with all Airport rules and regulations, including without limitation those pertaining to security. Any person who violates such rules may be subject to revocation of his/her access authorization. The failure of the Vendor or any subcontractor to complete any required services hereunder shall not be excused on account of the revocation for good cause of access authorization of any person.

The security status of the Airport is subject to change without notice. If the security status of the Airport changes at any time during the term of this Contract, the Vendor shall take immediate steps to comply with security modifications which occur as a result of the changed status. The Vendor may at any time obtain current information from the Airport Security Office regarding the Airport's security status in relation to the Vendor's operations at the Airport.

The Vendor shall return to the City at the expiration or termination of this Contract, or upon demand by the City, all access keys or access badges issued to it for any area of the Airport, whether or not restricted. If the Vendor fails to do so, the Consultant shall be liable to reimburse the City for all the City's costs for work required to prevent compromise of the Airport security system. The City may withhold funds in the amount of such costs from any amounts due and payable to the Vendor under this Contract.

LAWS, REGULATIONS, TAXES AND PERMITS

The Vendor shall procure all permits and licenses, pay all charges, taxes, and fees, and give all notices necessary and incidental to the due and lawful prosecution of the work. All costs thereof shall be deemed

to be included in the prices proposed for the work.

The Vendor, at all times, shall observe and comply with all federal, state, county, city and other laws, codes, ordinances, rules, and regulations in any manner affecting the conduct of the work.

Without limiting the foregoing, the Vendor shall establish appropriate procedures and controls so that services under this Contract will not be performed by using any alien who is not legally eligible for such employment under United States Immigration laws. Failure to comply with this condition satisfactorily may cause the City to terminate this Contract.

A.18 EMERGENCY PURCHASES:

The City reserves the right to purchase from other sources those items which are required on an emergency basis and cannot be supplied immediately by the vendor.

A.19 EMERGENCY 24-HOUR SERVICES:

Emergency twenty-four (24) hour service is to be provided by vendor at no additional cost. Below are the names and phone numbers of the individual(s) to contact for emergency service:

First Contact: Joe Slinger 303-304-9437

Second Contact: Tim Mantey 303-921-7566

This service requires a live telephone answering service with the capability of immediately contacting operating personnel at all times. Recorded telephone answering service is not acceptable.

A.20 COOPERATIVE PURCHASING:

The City encourages and participates in cooperative purchasing endeavors undertaken by or on behalf of other governmental jurisdictions, pursuant to Denver Revised Municipal Code Sec. 20-64.5. To the extent other governmental jurisdictions are legally able to participate in cooperative purchasing endeavors, the City supports such cooperative activities. Further, it is a specific requirement of this contract that pricing offered herein to the City may be offered by the vendor to any other governmental jurisdiction purchasing the same products.

Vendor(s) must contract directly with any interested governmental agency concerning the matters within this RFP.

A.21 VENDOR QUESTIONS AND REQUIREMENTS:

1. Describe your service level agreements for offsite storage and shredding services.

   All American Records Management, Inc. (AARM) has (4) services levels that we provide:

   - Next Day Service: Request by 4:00 PM deliver by 5:00 PM Next Day
   - Same Day Service: Request by 11:00 AM Deliver by 5:00 PM
   - Rush: Deliver within 2 hours of receipt of request
   - After Hours: Delivery requests outside normal business hours (8:00 AM to 5:00 PM)

The above referenced levels are for box retrieval and refile only. Authorized City users have credentials and can use our online portal to access inventory for delivery, pickups, and destruction requests.

All ongoing shredding services are scheduled for weekly, monthly, and twice a month service. Also, City and County of Denver employees can request special shredding projects:

- Special purge projects (destruction of boxes not part of the City and County of Denver inventory)
- Purge Bins (for special projects)
- Hard Drive Destruction
- CD Destruction
- LTO/DLT tape destruction
- Pallet pickup for direct destruction

2. Detail your company's approach to offsite storage and the protection measures you have instituted to ensure our content stays safe and damage free from various elements. All American Records Management, Inc. (AARM) provides personalized records storage, shredding and data protection services. AARM provides service locally 24/7 from local account management teams. AARM has the resources in place to provide cost effective solutions for all departments within the City and County of Denver.

Protection including security guards, physical barriers, alarms, access controls and video surveillance to prevent unauthorized access, theft or damage are active and in place at our records centers.

Johnson Master Security Control Panel Line cut monitor/
Manual Fire
Pull Glass break detectors in office areas Motion
detectors general office area
Overhead warehouse door contacts with magnets Door
Day alarm - all records center doors
entry doors Central station monitoring- Johnson Controls
Secure facility with intrusion and fire protection systems
Employee Confidentiality Agreement
Client Authorized User Form reviewed and submitted periodically. Client Web Authorized User Form reviewed and submitted periodically Standard operating procedures regarding authorized record request Standard operating procedures for secure pickup and delivery
Secured vehicles.
Authorized delivery signatures

File security pouches with numbered seals
Standard operating procedures regarding written record removal requests

- Fire detection/monitoring devices and fire suppression systems in compliance with NFPA 232.

  The concrete used in tilt-up panels meets the fire-resistance standards of even the most demanding building codes. For example, a 6.5 inch concrete wall offers a fire resistance rating of four hours or more. Tilt-up buildings offer real protection and safety for your storage documents. AARM has monitoring devices/motion detectors throughout the facility. Additionally, AARM is a compliant vendor and is in compliance with NFPA 232.

- Water/moisture detection and monitoring systems to prevent damage.

  AARM uses control valves in our facility. The system can shut down after a fire has been controlled, and for periodic maintenance and modification. In the AARM system a single shutoff valve is located at the point where the water supply enters the building. In the AARM building, the sprinkler system consists of multiple zones with a control valve for each. Control valves are in readily identified locations to assist responding emergency personnel.

  These shut down controls are locked in the open position. Keys for these locks are placed in a readily available location for emergency access. Detection alarms are installed on the control systems to notify the record center staff of an unauthorized system shut down.

- Temperature controlled.
  *Record Center only

- Humidity controlled.
  *Vault only

3. Do your facilities meet the National Archives and Records Administration's Facility Standards for Record Storage Facilities? How have you documented your compliance with these standards?

All American Records Management, Inc. (AARM) facilities meet the standards of the NARA. AARM has strict chain of custody methods, background checks, employee screenings and ongoing training to ensure security protocols are maintained. AARM utilizes the Envision DHS Worldwide Total Recall records management software program. This online program provides online management of boxes and files, including searching, tracking, and processing online requests. Also, it provides tailored solutions with advanced capabilities including:

- Client web server access with multiple user access
- Records retention scheduling for meeting regulatory requirements
- Extensive reporting capabilities for carton and file activity AARM

records centers also follow NARA building requirements:

- Quarterly sprinkler and alarm inspections
- Comprehensive fire protection, zoned detection, and wet and dry suppression systems
- Site outside 100-year flood plan
- Intrusion protection includes central station alarm, perimeter entry contact alarms, interior motion detectors, closed circuit TV, key/pad access card door systems, manual fire pulls, window glass break detectors.
- Fire extinguishers in place- inspected quarterly.
- Shelving professionally installed and loaded based on weight restrictions.
- Records centers provides emergency, holiday, after-hours access 365 days a year
- All required insurance coverage maintained and on file for review

* Attachment A (Disaster Recovery Policy) Attachment B (Privacy and Security Policy) provide extended documented compliance

4. Please describe your Disaster Recovery plan and procedures and are they available for review?

All American Records Management, Inc. (AARM) has created a Disaster Recovery Policy. The plan consists of a checklist of tasks to be executed by AARM managers and staff.
The purpose of our procedure's manual is to provide a guide to accomplish the following:

- Protect employees during hazardous life threating emergencies.
- Prevent damage to the properties, equipment, and customers' inventory during and emergency
- Provide and follow an action plan of Business Recovery/Resumption of business operations during an emergency

The AARM management team initiates a minimum of two sessions per year with individual managers and staff to familiarize/review/update emergency procedures contained in our plan. The management will, in turn, review the plan with our staff during regularly scheduled departmental meetings. The review plan is part of new employee orientations.

*Disaster Recovery Policy Attachment A provides extended documented compliance

5. What is your company's ability to provide a local person and easy contact method (Phone or Email) to deal with concerns, issues, or changes to shredding/storage needs for all 70+ City agencies and departments?

All American Records Management, Inc. (AARM) provides local dedicated account management to the City and County of Denver. Each department within the City and County of Denver has access to AARM's Manager of Account Services, Operations Manager, Business Development Manager, and

the President. Each department within the city has access via phone or email 24/7. AARM does not outsource customer service to another state or another country.

*AARM is the only locally owned company in Colorado. All company administration is in Centennial, CO.

Also, we have a customer service team in place to receive emails and can respond to authorized city department users.

6. Are you familiar with obtaining expanded (FBI, NSA, ECT) background checks for your employees' access to sensitive areas for shred bin service?

Yes, we are familiar with the extended background checks for All American Records Management, Inc. (AARM) employees' for access to sensitive areas for shred bin service.

7. Describe how your company maintains and ensures full compliance with HIPAA and the HITECH Act regulations.

All American Records Management (AARM) is compliant in all areas of regulatory compliance including HIPAA and HITEC. AARM has documented controls within our Disaster Contingency plan and our Privacy and Security Policy.

AARM has key requirements on how we maintain full compliance:

1. Administrative Safeguards-Documented operational processes and procedures for day-to-day operations, such as training, access, restrictions, managing employees and workflow to make sure information is managed securely and according to our policies.
   - Authorized Access- AARM has controls in place so information in our care is safeguarded. AARM uses security measures and tools such as employee identification badges, 24/7 surveillance and security on our owned buildings. Also, our online portal allows City and County employees to manage and control employee's authorization and access
   - Privacy and Security- AARM has established an all-inclusive method to protect the City and County of Denver's information. This includes designated security controls, safety and security procedures, audits (employees, records center, shredding plant) and enhanced training for employees and management.
   - Training and Staffing Practices- AARM has exceptional screening and training

programs:

- Complete background checks for new employees
- Screening of all drivers
- Employee training for correct handling of PHI
- CJIS training for all employees
- NAID training for all employees

2. Physical Safeguards: Physical security controls meant to protect AARM's information systems, as well as related buildings and equipment. Safeguard locks, key card access, keys, and protect against unauthorized physical intrusion.

- Fire protection security with an advanced fire suppression system with roof and in-rack sprinkler systems
- Stand-alone six-sided block filled concrete vault.
- FM-200 CO2 Fire Protection System (vault only)
- Climate and Humidity controls (vault only)
- Media container racks and gemtrac units
- ESFR Sprinkler System (semi-annual audits)
- Outdoor Siren/Indoor Siren
- Glass break detectors in office areas
- Motion detectors
- Overhead records center door contacts with magnets
- Quarterly records center audits to enforce compliance.

2a. Transportation: AARM has a secure fleet of transportation vehicles, collection trucks and mobile shred trucks:

- Secure pickup/delivery of City and County of Denver information
- Real time wireless scanning technology
- Vehicle process controls to prevent errors.
- Advanced vehicle security
- Proximity alarms to alert drivers.

3. Technical Safeguards- Security measures related to data information systems and other technologies, such as database security, AARM's network and user credentials (authorizations and passwords, to protect data from software invasion or attacks.) HIPAA requires that we are in compliance and AARM ensures that all measures are taken to protect

client information.

*Attachment A (Disaster Recovery Policy) Attachment B (Privacy and Security Policy)

8. Please detail your company's transition plan for getting your shredding containers distributed citywide to all agencies and departments and placed for service on day one if your company was awarded this contract.

All American Records Management currently has 555 bins that service the City and County of Denver and Denver International Airport. This was a coordinated delivery and AARM worked with the City and County of Denver employees to get all bins placed.

9. Discuss your company's approach to invoicing. Is your invoicing customizable to the City's needs?

Invoices can be customized to one invoice that reference multiple departments or individual invoices by department.

10. Propose as part of your response specific performance measures that may be used to develop a vendor performance management report card. Also provide any other data, criterion or methods that would be effective in measuring vendor performance over the life of this contract.

For shredding we can report back an estimated amount of paper collected and recycled by month, quarter, or year to show the environmental impact of recycling. For storage, we can generate a monthly, quarterly, or annual report showing the number of new boxes added, number of boxes destroyed or permanently removed, number of retrievals, refiles, bins delivered, bins serviced, and bins picked up along with total invoice amount during the selected period.

A.22 PRICING:

All prices quoted shall be firm and fixed for the specified initial one-year term of the contract.

A.23 PRICING ADJUSTMENTS:

All prices quoted regarding records management may be adjusted annually following the completion of the initial one year term upon request, however, only one (1) adjustment will be allowed per calendar year. Such requested adjustments shall be accompanied by a justification letter from the Vendor to the City Records Manager, with any required supporting documentation for the requested increase. Due to the number of agencies effected and City budget approvals, pricing increase requests must be submitted to the City no later than March 1st for consideration for addition to the following years' budget prior to their effective date.

In the event that the City's budgets have been capped and/or reduced, and/or City employee pay rates are frozen to budgetary constraints, then requested price increases may not be approved. All increases will be at the discretion of the City only.

Prices regarding future services after the initial one-year term shall be negotiated and mutually agreed upon by the Vendor and the City and County of Denver Technology Services Department, taking into consideration that adjusted increases in prices shall not exceed the inflation rate as defined by the Denver-Boulder-Greeley, CPI index for All Items on Table 1 for All Urban Consumers. If the CPI has a significant decline, the City reserves the right to request that the Vendor reduce their rates.

https://www.bls.gov/regions/mountain-plains/news-release/consumerpriceindex_denver.htm

A.24 Limitations of Liability

LIMITATIONS OF LIABILITY - AARM SHALL NOT BE LIABLE FOR ANY LOSS OR DAMAGE TO STORED MATERIAL, HOWEVER CAUSED, UNLESS SUCH LOSS OR DAMAGE RESULTED FROM THE FAILURE BY AARM TO EXERCISE SUCH CARE IN REGARD THERETO AS A REASONABLY CAREFUL OFF-SITE STORAGE PROVIDER WOULD EXERCISE IN LIKE CIRCUMSTANCES. AARM IS NOT RESPONSIBLE FOR THE REPAIR, REPLACEMENT OR RESTORATION OF LOST OR DAMAGED PROPERTY, SUBJECT TO THE CONDITIONS AND LIMITATIONS IMPOSED BY THIS AGREEMENT. ARM'S LIABILITY UNDER THIS AGREEMENT FOR ANY AND ALL CLAIMS, INCLUDING, WITHOUT LIMITATION, FOR LOSS, DAMAGE, OR DESTRUCTION TO PART OR ALL OF THE STORED MATERIAL STORED HEREUNDER, SHALL BE LIMITED TO: (A) FOR CLAIMS ARISING OUT OF MEDIA VAULTING SERVICES, AN AMOUNT NOT TO EXCEED THE REPLACEMENT COST OF THE MEDIA STORED HEREUNDER NOT TO EXCEED TEN DOLLARS U.S. PER ITEM; AND (B) FOR ALL OTHER CLAIMS, AN AMOUNT NOT TO EXCEED ONE DOLLAR U.S. PER ITEM STORED WITH AARM. IN NO EVENT SHALL AARM BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE OR SIMILAR TYPES OF DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOSS OF USE, NOTIFICATION REQUIREMENTS TO THIRD PARTIES UNDER STATE AND/OR FEDERAL LAW, LOST DATA, AND DATA AND/OR INFORMATION RECONSTRUCTION, REGARDLESS OF THE FORM OF THE CLAIM AND REGARDLESS OF WHETHER ANY SUCH DAMAGES WERE FORESEEABLE. Claims by Client for loss, damage, or destruction must be presented in writing to AARM within a reasonable time and in no event longer than sixty (60) days after Client is notified by AARM or otherwise receives notice that loss, damage or destruction to part or all of the Stored Material has occurred, whichever time is shorter. No action or suit may be maintained by Client or others against AARM for loss, damage or destruction of the Stored Material, unless timely written claim has been given as provided herein, and unless such action or suit is commenced within nine (9) months after Client is notified or otherwise receives notice that loss, damage or destruction to part or all of said Stored Material has occurred.

EXHIBIT B - CERTIFICATE OF INSURANCE

ALLAMER-02

PHOWARD

ACORD

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
10/25/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
Harold W. Wells & Son, Inc. 1 N 3rd Street Wilmington, NC 28401	PHONE (A/C, No, Ext): (910) 762-8551	FAX (A/C, No): (910) 254-9404
	E-MAIL ADDRESS: insurance@wellsins.com	

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : TransGuard Insurance Company of America Inc	28886
INSURER B : Starstone National Insurance	25496
INSURER C :	
INSURER D :	
INSURER E :	
INSURER F :	

INSURED

All American Records Management Inc
15580 E Hinsdale Circle
Centennial, CO 80112

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	$ 1,000,000
	CLAIMS-MADE X OCCUR	X	X	TCP0002165-02	12/1/2022	12/1/2023	DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 100,000
							MED EXP (Any one person)	$ 5,000
							PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 2,000,000
	X POLICY PRO-JECT LOC						PRODUCTS - COMP/OP AGG	$ 2,000,000
	OTHER:							$
A	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
	ANY AUTO						BODILY INJURY (Per person)	$
	OWNED AUTOS ONLY X SCHEDULED AUTOS	X	X	TCP0002165-02	12/1/2022	12/1/2023	BODILY INJURY (Per accident)	$
	X HIRED AUTOS ONLY X NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
								$
A	UMBRELLA LIAB X OCCUR						EACH OCCURRENCE	$ 5,000,000
	X EXCESS LIAB CLAIMS-MADE	X	X	TCU0001333-02	12/1/2022	12/1/2023	AGGREGATE	$ 5,000,000
	DED X RETENTION $ 10,000							$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N						PER STATUTE OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH)	N / A					E.L. EACH ACCIDENT	$
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$
							E.L. DISEASE - POLICY LIMIT	$
A	Cargo			TCP0002165-02	12/1/2022	12/1/2023	Any One Occurrence	50,000
B	Excess Liability			78100B225ALI	12/1/2022	12/1/2023	Excess over Transgu	5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Additional Named Insureds:
Hinsdale Properties LLC
Ponderosa Land & Investments LLC

Warehouse Legal Liability
$700,000 at 15580 E Hinsdale Circle, Centennial CO
$500,000 at 7246 S. Revere Parkway, Centennial CO
SEE ATTACHED ACORD 101

CERTIFICATE HOLDER

City and County of Denver
Department of Technology Services
201 W. Colfax Ave., Dept 301
Denver, CO 80202

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Cheri J. Sommer

AGENCY CUSTOMER ID: ALLAMER-02 PHOWARD

LOC #: 1

ADDITIONAL REMARKS SCHEDULE

AGENCY	NAMED INSURED
Harold W. Wells & Son, Inc.	All American Records Management Inc 15580 E Hinsdale Circle Centennial, CO 80112
POLICY NUMBER SEE PAGE 1	
CARRIER: SEE PAGE 1 / NAIC CODE: SEE P 1	EFFECTIVE DATE: SEE PAGE 1

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,

FORM NUMBER: ACORD 25 FORM TITLE: Certificate of Liability Insurance

Description of Operations/Locations/Vehicles:
$1,000 deductible except 2% for windstorm and/or hail

General Aggregate for General Liability is increased to $3,000,000 for each moving project.

Excess Liability applies with a limit of $5,000,000 per Occurrence/Aggregate in excess of the Transguard's $5,000,000 layer.

Contract #: TECHS-202369046
As required by written contract, The City and County of Denver, its Elected and Appointed Officials, Employees and Volunteers are additional insureds with regard to General Liability and Automobile Liability.

Cyber Liability
Houston Casualty Insurance
Policy # BZL697536
12/1/2022 to 12/1/2023
$1,000,000 Per Claim Cyber Liablity
$1,000,000 Aggregate Cyber Liability

Crime Insurance
Travelers Casualty and Surety Company of America
10/17/2023 to 10/17/2024
Policy # 107928872
Employee Theft - $1,000,000
Employee Theft of Client Property - $1,000,000
The City and County of Denver are Included as Loss Payee

From: Reittinger, Dulce
Sent: Thu, 24 Aug 2023 18:40:43 +0000
To: phoward@wellsins.com
Subject: ALL AMERICAN RECORDS MANAGEMEN - New Business Quote
Attachments: ALL_AMERICAN_RECORDS_MANAGEMEN__QUOTE_LETTER.pdf, ALL_AMERICAN_RECORDS_MANAGEMEN__SPECIMEN_ENDORSEMENTS.pdf

Hi Pam,

Thank you for providing the additional information! Attached are two quote options. The first option is for the requested coverage limits only while the second option includes all available crime coverages. Both have $1M limit with a $5k retention. I have also attached the Social Engineering and Telecom Fraud endorsements that would be applied to option 2 only as well as the Client Property Coverage endorsement.

One thing to note is that we are unable to add the City and County of Denver as additional insured. I can add a Joint Loss Payee endorsement but would need the loss payee's address.

Let me know if you have any questions/concerns or if any changes need to be made. Have a great rest of your day!

Best regards,

Dulce Reittinger | **Account Underwriter** | **BSI Private Non-Profit**
Travelers Bond & Specialty Insurance
11440 Carmel Commons Boulevard | Suite 205
Charlotte, NC 28226
W: 704.544.3732 | dreitti2@travelers.com
For information regarding our product offering, please click on the following link:
https://www.travelers.com/professional-liability-insurance

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 08/23/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
Doug Jones (for Paychex) c/o Artex Risk Solutions, Inc. P.O. Box 13838 Scottsdale, AZ 85267	PHONE (A/C, No, Ext): (888) 627-4735	FAX (A/C, No):
	E-MAIL ADDRESS: PEO_WorkComp@paychex.com	
	INSURER(S) AFFORDING COVERAGE	NAIC #
	INSURER A : American Zurich Insurance Company	40142
INSURED Paychex PEO Holdings, LLC Alt. Emp: All American Records Management Inc dba: All American Records Management 2054 Vista Parkway Suite 300 West Palm Beach, FL 33411	INSURER B :	
	INSURER C :	
	INSURER D :	
	INSURER E :	
	INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** 23FL9751154258 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	$
	☐ CLAIMS-MADE ☐ OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$
							MED EXP (Any one person)	$
							PERSONAL & ADV INJURY	$
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$
	☐ POLICY ☐ PRO-JECT ☐ LOC						PRODUCTS - COMP/OP AGG	$
	☐ OTHER:							$
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$
	☐ ANY AUTO						BODILY INJURY (Per person)	$
	☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
								$
	☐ UMBRELLA LIAB ☐ OCCUR						EACH OCCURRENCE	$
	☐ EXCESS LIAB ☐ CLAIMS-MADE						AGGREGATE	$
	☐ DED ☐ RETENTION $							$
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? Y/N: N **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A	X	WC 29-38-687-21	06/01/2023	06/01/2024	X PER STATUTE ☐ OTH-ER	
							E.L. EACH ACCIDENT	$ 2,000,000
							E.L. DISEASE - EA EMPLOYEE	$ 2,000,000
							E.L. DISEASE - POLICY LIMIT	$ 2,000,000
				Location Coverage Period:	06/01/2023	06/01/2024	**Client#** 100698-1	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Coverage is provided for only those co-employees of, but not subcontractors to: All American Records Management Inc dba: All American Records Management
15580 E Hinsdale Circle
Centennial, CO 80112

Contract #: TECHS-202369046

Endorsements: Waiver of Subrogation

CERTIFICATE HOLDER

City and County of Denver Department of Technology Services
201 W. Colfax Ave Dept. 301
Denver, CO 80202

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

WORKERS' COMPENSATION AND EMPLOYERS' LIABILITY INSURANCE POLICY **WC 00 03 13**

(Ed. 4-84)

WAIVER OF OUR RIGHT TO RECOVER FROM OTHERS ENDORSEMENT

We have the right to recover our payments from anyone liable for an injury covered by this policy. We will not enforce our right against the person or organization named in the Schedule. (This agreement applies only to the extent that you perform work under a written contract that requires you to obtain this agreement from us.)

This agreement shall not operate directly or indirectly to benefit anyone not named in the Schedule.

Schedule

IN FAVOR OF:

City and County of Denver Department of Technology Services
201 W. Colfax Ave Dept. 301
Denver, CO 80202

WORK PERFORMED BY CO-EMPLOYEES OF:

All American Records Management Inc dba: All American Records Management
15580 E Hinsdale Circle
Centennial, CO 80112

ON THE FOLLOWING PROJECT:

Contract #: TECHS-202369046

FEE FOR THIS WAIVER IS:

Premium will be waived

This endorsement changes the policy to which it is attached and is effective on the date issued unless otherwise stated.

(The information below is required only when this endorsement is issued subsequent to preparation of the policy.)

Endorsement Effective: 08/21/2023 Policy No: WC 29-38-687-21 Endorsement No:

Insured: Paychex PEO Holdings, LLC Alt. Emp: All American Records Management Inc dba: Premium: $

Insurance Company: American Zurich Insurance Company Countersigned By:

Authorized Representative

Preface

The purpose of this manual is to acquaint ***AARM*** managers and staff with procedures and tasks to be accomplished prior, during, and following a disaster, and more specifically, a tornado.

The following section is a checklist of tasks to be performed by the AARM managers and staff. During preparations, the Operations Manager will intervene in reassigning available employees and managers to accomplish all the stated tasks.

The use and familiarization of the plan shall be the responsibilities of all managers. It is suggested that the managers brief all employees to ensure their understanding of the plan at the onset of the tornado season (May, June and July). Each manager in turn should review the plan with staff at least three (3) times during the tornado season, preferably May, June, and July.

Remember: A Disaster Plan is:

A comprehensive, consistent statement of all of the actions to be taken before, during and after a disaster (or contingency), along with documented, tested procedures which, if followed, will ensure the availability of critical resources and facilitate maintaining the continuity of operations in a contingency situation.

Remember: Disasters can be Community Wide - Area Wide - Business Related - Any Business Interruption Can Be Disastrous!

Natural	Earthquakes	Fires
	Tornadoes	Floods
	Lightning	Hail storms
Technical	Power Outages	Telecommunication Outages
	Gas Leaks	Software/Hardware Failures
	Explosions	Hazardous Materials
Human	Lost or misfiled documents (unintentional or from disgruntled employees)	
	Sabotage	Theft
	Bombs	Computer Viruses
	Riots	Lawsuits

Contents

I. Executive Summary

The purpose of this procedures manual is to provide the ***AARM*** managers and staff a specific guide to accomplish the following:

- ⇨ Protect employees during hazardous or life-threatening emergencies.
- ⇨ Protect/prevent/mitigate damage to the properties, equipment, and customers' deposits during emergencies.
- ⇨ Provide an action plan for all staff to follow in making preparations for emergencies.
- ⇨ Provide an action plan of Business Recovery/Resumption of business operations during an emergency.
- ⇨ Provide a guide in assessing damages to said properties, equipment and customers' deposits.

All managers should possess a copy and be familiar with the Emergency Procedures Manual.

The Corporate Management will initiate a minimum of two sessions per year with individual managers and staff to familiarize/review/update emergency procedures contained in this plan. Each manager will, in turn, review the plan with their respective staff during regularly scheduled departmental meetings (minimum of three times per year). The review of the plan should be a part of new employee orientations within their respective departments. The following should be included in a Disaster Plan review with employees:

- ⇨ Protection during Life-Threatening Emergencies such as fires, tornados and other disasters
- ⇨ Returning and Resumption of work following a major disaster.
- ⇨ Personal and family protection for employees at their home.
- ⇨ Review of specific disaster preparedness and recovery responsibilities as assigned by respective department managers.

Policy Statements/Commitments

- ⇨ Minimize disruption of service to your customers and maintain an acceptable service level until fully operational.

- ⇨ Minimize financial losses to your facility and to ***AARM*** customers.

- ⇨ Ensure timely resumption of operations

- ⇨ Loss of business coverage

- ⇨ Commitment to plan testing, evaluating and updating.

II. DISASTER PRE-PLANNING

Company Responsibilities

II. DISASTER PRE-PLANNING

DISASTER TEAMS ASSIGNMENTS

CORPORATE MANAGEMENT TEAM

Responsible for all decision making and contacts with disaster teams, customers, employees, public relations/media, insurance agents.

Corporate Disaster Team:

General Manager Disaster Leader
Operations Manager
Warehouse Manager
Administrative Manager
Communications Specialist
Information Systems Specialist
Human Resources Specialist
Purchasing Specialist
Real Estate Specialist
Safety Specialist
Chief Financial Office - Corporate
Corporate Staff where needed

COMMUNICATIONS TEAM

Responsible for all communications, telephone systems, long distance lines, fax machine, modem connections.

Branch: Communications Specialist

OFFICE FACILITIES TEAM

Responsible for all office requirements, customer service requests, office equipment (copier and fax supplies, office supplies of forms, bar code labels, ribbons, computer paper, typewriter, calculators, billing requirements, desk supplies),

Branch: Purchasing Specialist

DATA PROCESSING TEAM

Responsible for all data processing requirements, hardware, software, and backups (networks, personal computers, all printers, modems, power supply, twinax cables, tape backup devices)

Branch: Information Systems Specialist

WAREHOUSING TEAM

Responsible for securing warehouse facility, security alarms, sprinkler, perimeter.

Branch: Operations Manager, Leader
Warehouse Manager
Real Estate Specialist
Warehouse staff

DISASTER PRE-PLANNING

OFFICE FACILITIES TEAM

1. Maintain and update disaster contingency planning manual.

2. Current telephone number and address of all employees and home office contacts should be maintained in disaster contingency planning notebook. At each revision of employee information, copies are to be distributed as follows: one each to included in Disaster Contingency Planning Manual for master office copy, General Manager's home copy, Operations Manager's home and office copy, Administrative Supervisor's home and office copy.

3. For inventory and insurance purposes, maintain current fixed assets of office equipment, including model and serial numbers (include photos if possible):
   - Typewriter
   - Copier
   - Fax Machine
   - Microfiche Equipment
   - Office Furniture/Fixtures
   - Work Station Panels

4. Maintain floor plan of furniture, fixture, communications.

5. Continue procedure to have all signed storage agreements placed in vault in Corporate headquarters.

6. All vital records should be clearly identified with fluorescent disaster planning label, and executed pre-authorization statement identifying vital records should be placed in customer file.

7. Daily backup procedures in place, with extra media available to produce extra backup prior to emergency evacuation.

8. Notify Information Systems specialist and software vendor of pending disaster. Local WAN weekly backup mailed to offsite.

9. Maintain current master report on customer deposits.

10. Current listing of customers names, contacts, addresses, telephone numbers.

11. Develop telephone reporting tree.

12. Develop escape routes in case of fire. Determine two escape routes from each room. Select area where employees can meet after escaping and ensure everyone accounted for.

DISASTER PRE-PLANNING (continued)

WAREHOUSING TEAM

1. For inventory and insurance purposes, maintain current inventory including model and serial number on equipment (include photos if possible):
   Scissor Lifts
   Pallet Jacks
   Fork Lifts
   Delivery Equipment (Van/Panel Truck)
   Dollies/Handcarts (2 wheels/4 wheels)
   Alarm Equipment
   Fire Extinguisher/Hoses

2. Fire extinguisher should be tested and refilled, if necessary, as required for safety - minimum every six months. All warehouse and office employees should be trained on use of fire extinguisher, including new employees during orientation, and placement should be well marked for quick access.

3. Water and electric shut-off valves should be well marked and employees trained on use. Keys for locks should be easily accessible.

4. All work in progress should be palletized.

5. New racking material should be anchored to flooring before shelving begins. Flooring built-up bottom shelf?

6. Warehouse/perimeter maintenance:
   Roof Condition and Flashings: Leaks? Cracks?
   Eaves, Gutters, Downspout? Cleaned regularly?
   Skylights? Caulking sound? Trees trimmed?
   Air Conditioning checked regularly?
   Exits unobstructed?
   Annual Fire Marshall visit
   Wiring Condition? Overloading?
   Housekeeping: Safe storage practices closets? Trash removal? Cleaning supplies/flammable storage?

7. Develop telephone reporting tree.

8. Develop escape routes in case of fire. Determine two escape routes from each room. Select area where employees can meet after escaping and ensure everyone accounted for.

DISASTER PRE-PLANNING (CONTINUED)

Warehouse team should prepare the following building/site maps and directions:

- Utility shut-offs
- Water hydrants
- Water main valves
- Water lines
- Gas main valves
- Gas lines
- Electrical cutoffs
- Electrical substations
- Storm drains
- Sewer lines
- Location of each building (include name of building and address)
- Floor plans
- Alarm and enunciators
- Fire extinguishers
- Fire suppression systems
- Exits
- Stairways
- Designated escape routes
- Restricted areas
- Hazardous materials (including cleaning supplies and chemicals)
- High-value items

DISASTER PRE-PLANNING (continued)

DATA PROCESSING TEAM

1. For inventory and insurance purposes, maintain current fixed assets of computer equipment, including model and serial numbers (include photos if possible):

Monitors	Processors
Printers	Modems
Keyboards	Mouse
Tape Backup Device	Power Supply

2. Develop telephone reporting tree.

3. Vendor association established for assistance in recovery efforts and hot-site assistance.

COMMUNICATIONS TEAM

1. For inventory and insurance purposes, maintain current inventory of all telephone equipment, including model and serial numbers if available. All incoming and outgoing numbers should be outlined with purpose, including fax, data, remote access and remote scanning lines.

2. Vendor association established for assistance in recovery efforts and hot site assistance.

3. Maintain "remote access for call forwarding" feature for use during disaster.

4. Develop telephone reporting tree.

MANAGEMENT TEAM

1. Maintain current media contacts and telephone numbers for distributing news releases after disaster.

2. Insurance policy in place for business loss - annual insurance review, new equipment added to policy, federal disaster relief procedures, eligibility?

3. Decide role in community disaster.

4. Develop telephone reporting tree.

5. Arrange pre-registration with emergency response vendors.

SAMPLE

TORNADO SCHEDULE ALERT

To: All AARM Customers

From: General Manager

Date: Current

Re: **TORNADO SCHEDULE**

As you all know, a Tornado Warning has been posted for the Centennial area. It appears the path of the storm will be north of the Denver Metro area, although a clear path cannot be predicted at this time.

We do expect to receive some severe weather in the Centennial area as a result of this hurricane. For that reason, we are posting the following schedule change.

1. All normal scheduled or on-call pickup and delivery service will be suspended from 12:00 noon Thursday to 12:00 noon Friday. This suspension may need to be lifted or extended on the arrival and severity of the storm.

2. Emergency pickups or relocation of product will be available on a first call, first served basis from 8:00 am Wednesday to 10:00 am Thursday.

3. The warehouse facility will be secured and shutdown as of 4:00 pm Thursday, June 5, 2009. This schedule may be lifted or extended depending on the arrival and severity of the storm.

AARM will be prepared to be back in normal operation mode as soon as this weather crisis passes. Thank you for your patience during this service interruption.

SAMPLE

MEMORANDUM

To: **All employees**

From: **Human Resources**

Date: **Current**

Re: **Preparation for Tornado/Storm**

At this time, we are not aware of what course the storm will take. You are released at 3:30 to go home and take care of your personal needs.

POLICY FOR REPORTING TO WORK THURSDAY AND FRIDAY:

1. **You should report to work unless conditions prohibit you.**

2. **In case you are in need of emergency assistance, we will try to respond to you. We are concerned for your personal safety. By keeping in touch with your supervisor, we can keep a head count and help locate anyone who might be unaccounted for.**

3. **If you are not in an area that has been evacuated or in an emergency situation, we will need all personnel to report to work to help others that are in need as well as securing all our work areas.**

Keep tuned to your radio for important updates and announcements. AARM, along with other companies will be broadcasting on radio station KOA 850 AM.

Vendor Responsibilities

1) Communications – (Telephone Company) agreement for "Remote Activation of Call Forwarding" Feature - Customer service will be available once warehouse facility re-opens - Arrangements confirmed with parent company for forwarding option.

2) Office Supplies/Forms - Available through parent company which provides master supply operations.

3) Computer Hot Site - Available through parent company which provides technical support - backups stored in vault

III. DISASTER READINESS

GENERAL MANAGER RESPONSIBILITIES:

- ⇨ General Manager should begin tracking of tornado. Begin monitoring weather channels or NOAA radio weather alert channel for sudden shifts or change, and current position updates.

- ⇨ Mandatory attendance of managers meeting will immediately follow posting of a "Tornado Warning". This will be approximately 30 minutes since announcement. Get final authorization from executive management for authorization to implement "Disaster Readiness and Relocation Program". Activate "Disaster Readiness Teams" and disaster "Alert" file should be updated immediately for latest information. Previously signed pack and transport agreements should be initiated. Establish scope of anticipated removals and begin transportation to designated alternate sites.

- ⇨ Scheduled briefings for all department management will be necessary prior to warehouse facility closing. As part of the final briefings, prior to the storm, the establishment of a reopening staff needs to be accomplished. Schedule a back-up employee to report following the storms passage.

- ⇨ Adjust warehouse facility business hours as needed and determine from weather forecasts closing time of AARM. Closing time needs to be gauged carefully -- usually when customers stop calling or strong winds make driving difficult - disseminate closing time to all staff.

- ⇨ Several hours will be needed to completely secure warehouse facility for closing. Need to be overly cautious. Once a closing time has been decided, staff will be allowed ample time to secure facility and get home safely.

- ⇨ If possible, one employees will be designated to stay in the building through the storm. (Preference will be given to employees who live nearby and/or have minimal family obligations.) Have employees assemble a survival kit (See emergency shopping list).

- ⇨ Make sure an up-to-date listing of employee telephone numbers and addresses is available to all management. Find out where all employees plan to stay during storm in case they do not report back to work afterwards. May need to send someone to check on them to ensure they are not trapped.

- ⇨ Copy of current account master should produced for all management staff.

- ⇨ Report closing hour to corporate office. Insure vendors know of warehouse closing and that all plans for warehouse deliveries have been completed or cancelled.

- ⇨ Since ATM(s) and other credit card devices will be impaired or inoperative, make arrangements with parent company for employees to receive pay in cash, immediately after the storm.

- ⇨ Check with parent company for location of one or two portable generator units and designate employees responsible for safe-guarding units, transporting them to the premises after the disaster, and ensuring sufficient fuel arrangements are made. Consider doing the same for dehumidifiers, portable toilets. Arrange for deployment of "AARM Grocery Store" housed in training trailer.

- ⇨ Contact nearby hotel to be used in housing any employees whose family may be rendered homeless as a result of the disaster.

DISASTER READINESS

MANAGEMENT TEAM

1. Distribute disaster plan to each disaster team leader with master copy placed in secure location.

2. Advise team members of potential disaster and class and place on alert.

3. Telephone tree updated and received from General Manager and beeper issued to team leaders.

4. Insurance documents secured.

5. Make arrangements with parent company to receive backups
   (computer down over 7 days - cold site)
   (computer down less than 7 days - hot site)

6. Make decision for alternate headquarters.

7. Moving/relocating plans for alternate sites.

8. Determine total space requirements in the event relocation is necessary.

9. Place employees from other subsidiaries on "Readiness Notice". Get employee telephone numbers from personnel department.

10. Place temporary staffing on "Readiness Notice".

COMMUNICATION TEAM

1. Copy inventory and fixed assets listing of all telephone equipment. Place updated list in each team members disaster manual, with copy in secure location and possibly mailed off-site (photos if available).

2. Telephone equipment should be secured - unplugged and placed in vault.

3. Telephone tree updated.

4. Discuss telephone remote activation process - be sure correct telephone numbers are published along with pin activation numbers. Establish individual responsible, along with backup, for activation process.

5. Create updated directory of mobile phones and beepers in place and operational. Decide ownership of all equipment and provide numbers to staff.

OFFICE FACILITIES TEAM

1. Copy inventory and fixed assets listing of all furniture, fixtures, office equipment. Place updated list in each team members disaster manual with copy in secure location and possibly mailed off-site (photos if available).

2. Each employee should have updated employee security badge for warehouse facility before they leave premise, for easy identification by all authorities once disaster recovery process has begun. Team Leaders should be issued special identification badges.

3. Arrange for immediate security guard following disaster - protection of organization's information, facilities, furnishings, equipment, and materials.

4. Place work in progress material in secure location.

5. Designate an employee to be responsible for moving vital office files/ records to secure location and all other documents should be moved to safe areas of the building away from glass. All desktop papers and materials should be removed and properly stored in file cabinets or in the vault.

6. Supplies should be placed in secure location. Copy and fax paper, labels, stationary, general office supplies.

7. Contact customers with emergency beeper telephone number.

8. All contracts and agreements should be placed in secure location, including warehouse agreements.

9. Update telephone tree and distribute.

10. Place local telephone book in secure location.

11. All PC CD’s should be placed in secure location.

12. Prepare latest account receivable listing and place in secure location. . Checks should be deposited or placed in secure location. All cash should be deposited before warehouse closing. Also make arrangements with parent company to obtain cash after the storm. Cash advances may be needed by employees for housing, repairs or miscellaneous expenses. If power is out, it may be difficult to obtain cash.

13. Billing profiles of rates and charges should be placed in secure location.

14. Place blanket purchase orders in secure location.

15. Blanket purchase orders should be given to disaster leader.

16. Federal and sales tax certificates copied and placed in disaster manual, original on file at corporate office.

17. Check with personnel regarding payroll records and methods for paying employees after disaster.

18. Check with parent company to ensure all incorporation papers are safeguarded.

19. Check with alternate sites for backup of supplies, equipment.

20. All windows, window coverings, and doors should be closed. Designate employee to be responsible for taping/boarding windows.

21. Furniture should be covered with couch wrapping for protection from water damage.

22. Ensure all electric connections are shut down prior to the storm's arrival.

WAREHOUSING TEAM

1. Inventory and stock needed recovery supplies. Boost orders/supplies of batteries, flashlights, candles, sterno, first aid supplies, etc. Assist with stockpiling canned food and water for employees use after storm.

2. Begin operations for "Disaster Readiness and Relocation Program". Identify any product requested to be relocated in "Alert" files. Contact temporary staffing for extra help and establish requirements for labor before and after storm.

3. Transport warehouse vital records.

4. Telephone tree updated.

5. Secure perimeter and vehicles before closing facility.

6. Secure overhead doors with pads to prevent water entry.

DATA PROCESSING TEAM

1. Before exiting building, awaiting disaster, all computer, fax, and telephone equipment should be placed in secure location. Disconnect power cords from twinax cables.

2. Help establish computer and spacing requirements for hot site at parent company.

3. Unplug and disconnect all outlets.

4. Telephone tree updated.

5. All original software and manuals placed in vault.

6. Backups should be created and placed in secure location for all systems - main network, personal pc's and laptops. Hard copy report should be placed in secure location for manual retrieval efforts.

DISASTER SUPPLIES REQUIRED

Water Hoses
Mops, Brooms
Dehumidifiers
Buckets
Forms, Ribbons, Labels, Paper
First Aid Kit
Flashlights
Batteries
Gloves
Heavy Plastic Sheeting
Overalls
Blankets
Book Carts
Camera Film
Calculators and Paper
Copier and Paper
Extension Cords
Fans
Fire Extinguisher
Fungicides
Generator (Portable and Fuel)
Forklift and Propane
Paper Towels (Not Colored)
Pencils
Pens (Ball Point)
Plastic Milk Crates]
Plastic Trash Bags
Scissors
Sponges
Staplers and Non-Rusting Staples
String
Waterproof Utility and Packaging Tape
Wiping Cloths
Unpainted Newspaper
Hand Trucks
Hard Hats
Ladders
Mops
Pagers - Beepers
Pallets
Radios and Batteries
Wet/Dry Vacuum
Chairs
File Cabinets
Work Tables
Waterproof Markers
Lint Free Cloths
Chemicals for Preserving
Microfilm/Microfiche
Utility Knives
One Tablet of 9x12 Sheets
Tool Kit including Screwdrivers
Wire Cutters for Locks
Shovel
Two-Way Radios
Adhesive Labels
Crowbar
Typewriters
Safety Glasses
Spot lights
Trash cans (large and small)

IV. DISASTER RECOVERY

DAMAGE ASSESSMENT/RECOVERY:

Following local news media's announcements on the storms passing and an "all clear notice" the General Manager will attempt to establish contact with Disaster Team Leaders to visit site and assess damages. Much will depend on the amount of damage and debris as to the feasibility of opening the facility.

MANAGEMENT TEAM

1. Team leaders to assess disaster and assemble disaster teams.

2. Arrange for building admittance-being sure safety and well-being of staff has been provided for.

3. Hot or cold site needed?

4. Arrange relocation to alternate site.

5. Prepare public relations statement to media.

6, Advise customers as to present business position.

7. Get approval from authorities to re-enter building (be sure to also take into consideration health hazards).

8. Normalization important - don't allow employees to talk about disaster and resume wearing normal business attire as quickly as possible.

9. Expenses cleared through management.

DAMAGE ASSESSMENT REPORT:

DAMAGE ASSESSMENT REPORT

For extent of damage, enter the number appropriate for the degree of damage.

0 - None
1 - Minor
2 - Major
3 - Destroyed

A. PHYSICAL PLANT DAMAGE

Roof

_____ Describe damage briefly:_____

_____

_____

Air Conditioning

_____ Describe damage briefly:_____

_____

_____

Windows and Doors

_____ Describe damage briefly:_____

_____

_____

Walls/Signs/Parking Lot

_____ Describe damage briefly:_____

_____

_____

Flooding Damage - Height of Water

_____ feet, _____ inches. **Note**: Look for water marks if water has gone down.

B. UTILITIES:

Electrical Power: _____ ON _____ OFF

When did power fail? Date/Time: _____ _____ a.m./p.m. (circle)
When did power resume? Date/Time: _____ _____ a.m./p.m. (circle)

Natural Gas

Meter Damage	___ YES	___ NO
Damage to Lines	___ YES	___ NO
Is it leaking?	___ YES	___ NO

C. MERCHANDISE / SUPPLIES INVENTORY:

See attached vendor listing for contacts, and products.

D. EQUIPMENT DAMAGE:

For extent of damage, enter the number appropriate for the degree of damage.

0 - None
1 - Minor
2 - Major
3 - Destroyed

E. PERSONNEL ASSESSMENT:

Warehouse reopening date: _____ Time: _____

New revised hours (if changed) _____

List known problems with employees:

Employees name: Problem:

_____

_____

_____

_____

_____

1. Reopening staff. This staff, which was established by general manager just prior to landfall, will now be arriving at the location to make arrangement for opening the location for business.

2. Should sufficient number of staff be available to open location, determine location open time.

DISASTER RECOVERY

DATA PROCESSING TEAM

1. Assess damage and assemble disaster team.

2. Data Processing operational ASAP!

3. Contact necessary vendors for replacement or repair.

WAREHOUSING TEAM

1. Assess damage and assemble disaster team.

2. Must use protective gear (rubber boots, gloves, splash suit, hard hats) before entering building - possibility of bacteria, gasoline, PCB's asbestos, etc.

3. Limit extent of damage and prevent the escalation of disaster if possible.

4. Determine:
   A) Unsalvageable
   B) Salvageable - No Damage

5. Must have controlled demolition - inventoried and photographed for insurance purposes.

6. Rebox material, if required, onto numbered pallets. Make inventory of pallet – identification number, location number, and description. Load pallets and move to designated alternative warehouse; unload. Keep pallets in order with working space between.

7. Once shelving replaced, load product/pallets as fast as possible in new locations - with computer index of old location, new location, and identification number. Verifying contents is last step of recovery.

8. Contact restoration vendor and follow guidelines, as approved by Customer.

9. Arrange for vital records to be returned to facility ASAP!

10. Check sprinkler, air conditioning, and alarm systems

DISASTER RECOVERY (continued)

COMMUNICATIONS TEAM

1. Assess damage and assemble disaster team

2. Re-establish communications - outside lines first priority. Remote activation of telephone lines for customer/employee contact.

OFFICE FACILITIES TEAM

1. Assess damage and assemble disaster team.

2. Pickup all contents stored in secure location and begin operations in designated area.

3. Setup customer service area ASAP!

4. Contact necessary vendors for replacement or repair.

V. EMPLOYEE RETENTION PLAN AND CONTINUANCE OF BUSINESS:

Disasters that cause wide spread property damage and loss of normal communication can cause employees to be delayed or not return to employment.

A. MANPOWER SHORTAGE PREVENTION:

The following methods and procedures will prevent a severe manpower shortage (employee absence) and ensure expedient business resumption.

a. Employees briefed on first day of employment and/or twice a year.
b. Employees report to their respective department manager (physical visit to department premises) or if premises are damaged at ___(provide area)___, during the hours of _____ immediately following the occurrence when traveling is deemed to be safe.
c. Upon reporting to the premises, the administrative unit or department managers, as designated by the administrative unit will provide briefing to include:

    1. Assessment of disaster
    2. Needs of employees
    3. Reassurance of employment
    4. Date and time to report back to work
    5. Any specific job assignments to help with recovery and resumption of business.
    6. Referrals - should employees have severe disaster caused needs, then the administrative unit and department managers will determine available Disaster Assistance resources to meet their needs. (Allow time off for employee to apply, to determine resource, to consult with local media and/or the American Red Cross to receive assistance.

d. Administrative unit instructs department managers to coordinate, with their respective staff, recovery plans for their department, as contained in the plan.
e. Assessment of damage to premises.
f. Determine safety of premises for business resumption or, if necessary, search for an alternative place of business.
g. Once alternative location is found, administrative unit will brief employees.
h. Administrative unit determine times when business will resume - partial or full time.

B. DISASTER ASSISTANCE FOR EMPLOYEES:

In the process of recovering the business operation to full staff after a large scale disaster, it will be necessary for the Administrative Unit to request department managers to interview returning employees about their disaster losses including their respective families and personal property losses. The following questions can be asked by Administrative Unit and managers:

1. Injuries to employees and family members?
2. Displacement of home?
3. Other significant disaster caused loss which would require leave time from employment?
4. Time needed by employee to rectify/recover from loss?
5. Specific emergency help needed by employee (i.e., food, shelter, clothing, etc.)?

Once personal losses of employees are determined, managers should grant leave time as needed, and establish emergency shifts and schedules for employees to recover operations and resume business operations.

For help to employee severely affected by disaster, managers can make referrals of employees to American Red Cross Center(s) which will open three to five days following a large disaster occurrence. Administrative Unit and managers can attempt to contact Red Cross locally or receive updated announcements by media, radio, newspapers, and fliers, as to where and when service centers will open. From Red Cross centers, employees will find further recovery assistance, distribution of supplies, food, and medical services in the immediate vicinity.

AFTERMATH -- WHAT IT WILL BE LIKE:

Following the passage of the storm, or any disaster, it will be the responsibility of each employee to contact the location (physically drop by) to determine the time to report to work.

Despite all your preparations, you may find your location damaged beyond opening and totally unsafe. If the building and equipment have suffered minimal damage, other obstacles will come to light. You may have a difficult time obtaining additional fuel because some fuel is pumped by electric pumps, and if the power is turned off at the fuel station, it can't be pumped. You may need to request supplies fuel from outside the affected areas.

It is very likely that you'll need to throw out spoiled perishables starting the day after the storm, but bear in mind that there may not be garbage service for a week or so because roads are blocked by fallen trees or downed power lines. By the same token, you may not be able to

receive shipments for several days because of the same reason. Once again, your own creativity may be your key to success.

If your water or sewer service has been interrupted, your rest rooms will not be functional. Since functional restrooms are required by law, you may be legally prevented from opening until you can make arrangements for portable toilets.

Water service may continue but the water may be declared unsanitary due to contamination of the supply. In this case, food preparation services may need to switch to using bottled water for washing and cooking purposes. Water fountains and soda fountains connected to tap water will need to be shut off.

Because there is such a wide range of scenarios, our guidelines will not be able to address every contingency. Each location/department manager will need to formulate his or her own recovery plan to prepare for the disaster.

Warehouse facility reopening for cleanup and recovery:

Note: Managers will need to determine time staff will need in order to clean up, repair, and reorder supplies.

1. Following the evaluation of the Damage Assessment report and return of employees, a complete log of hours worked should be maintained on paper if power is down. Also, any extra costs to reopen location should be documented.

2. For minor damage to the warehouse, the general manager has authority to secure proper assistance to effect repairs.

3. For damage to equipment, the general manager may make contact with day-to-day repair resources, i.e., computer repair, copier repair, cash register repair, etc. This will largely depend on the manager's experience and extent of damages in his or her area.

VI. EMERGENCY TELEPHONE NUMBERS/ADDRESSES

EMPLOYEES

CUSTOMERS

SUPPLIERS

AARM RESOURCES
LOCAL/STATEWIDE

NATIONAL NETWORK

AARM
EMPLOYEE HOME ADDRESS LIST

General Manager
7937 Renault Drive
Parker, CO 80134
Phone: 720-573-1363
Cell: 720-591-2991

Warehouse Manager
7535 S. Jasmine Ct.
Centennial, CO 80112
Phone: 303-771-1196
Cell: 303-241-3249

Administrative Manager

11537 Sedgemoore Dr., N.
Littleton, CO 80124
Phone: 268-8212
Car: 631-3985

Assistant Warehouse Manager
12119 Blackfoot Trail
Castle Rock, CO 80134
Phone: 303-262-115
Cell: 303-838-6739

Account Executive
2172 Rothbury Dr.
Golden, CO 80401
Phone: 303-786-6060

The AARM Companies
BRANCH TELEPHONE NUMBERS

VENDORS

(Each branch should identify local contacts for the following type businesses.

ALARM SERVICE
BANDING MATERIAL
BUILDING CONTRACTOR
CABLING-NETWORK/CPC
PHONE
CLEANING SERVICES
COMPUTER HARDWARD
COPIER
COURIER SERVICES
ELECTRIC
ELECTRIC/EXHAUST FANS
ELECTRONIC
FACSIMILE TRANSMISSION
FIRE EQUIPMENT
FURNITURE
GENERAL CONTRACTOR
HEAT/AIR
LABELS
LOCKING SYSTEM
LUMBER
MISCELLANEOUS (FANS)
OFFICE SUPPLIES
PAINT
PEST CONTROL
PLUMBING

PRINTING
RACKING
RESTORATION SERVICES
SCISSORLIFT RENTAL
SECURITY
SOFTWARE
SPRINKLER SYSTEM
TELEPHONE SYSTEM
TRAILER RENTAL
TRUCK RENTAL
UPS SOURCE
WASTE DISPOSAL

VII. HAZARD - SPECIFIC INFORMATION

A. Fire

Fire is one of the most common disasters. Fire causes more deaths than any other type of disaster. Smoke detectors should be checked periodically to help prevent deaths in a fire.

B. Floods

Prolonged rainfall over several days can cause a river or stream to overflow and flood the surrounding area. A flash flood can be from a broken dam or levee or after intense rainfall of one inch (or more) per hour.

The rule for being safe is simple: HEAD FOR HIGH GROUND AND STAY AWAY FROM THE WATER!

FLOOD WATCH: means a flood is possible in your area.

FLOOD WARNING: means flooding is already occurring or will soon occur in your area.

EVACUATION:

Local government may recommend evacuation of specific areas along the coast. Evacuation orders should be taken seriously. If your business is in an evacuation zone, you should close as soon as possible after the announcement. If your staff lives in an evacuation zone, they should be released immediately.

If your warehouse facility is not in an evacuation zone, business will continue to be brisk until the public perceives the danger to be too great to venture out. This may mean that you'll want to extend your hours beyond normal closing time, or you may want to close early. Your customers will be your guide here. You may also be forced to close early due to a power failure.

Since a power failure is very likely, you will want to take special precautions after closing. As many perishable foods (except produce) as possible should be stored in the appropriate freezer or cooler. Gas should be cut off prior to departure, and circuit breakers for all compressors should be turned off if the power has already failed.

Inventory near the front windows should be moved to a safe location in case of glass breakage and to avoid theft. One or two management personnel should be designated to remain in the warehouse facility after closing, provided evacuation has not been recommended. It will be their responsibility to activate all of the

necessary precautions in the event of a power failure, and to protect the warehouse facility from looting.

C. HURRICANES:

1. HURRICANE TERMINOLOGY:

GALE WARNING - A warning associated with winds of 39 to 54 mph.

HURRICANE - An intense tropical weather system with a well defined circulation and a sustained wind speed of 74 mph or higher.

WINDS

Category 1	74-95 mph
Category 2	96-110 mph
Category 3	111-130 mph
Category 4	131-155 mph
Category 5	above 155 mph

Hurricanes are tropical cyclones in which winds reach a constant speed of at least 75 mph and may gust up to 200 mph. Their heavy bands of spiral clouds may cover an area of several hundred miles in diameter and generate torrential rains and tornadoes.

The eye of the hurricane is deceptively calm, almost free of clouds, with light winds and warm temperatures. If the eye passes over your area, only half of the storm has passed, the latter half has yet to come.

As the hurricane moves over the ocean, a dome of water - the storm surge - forms in the middle. **The storm surge is the most dangerous part of the hurricane.** The storm surge is responsible for 9 out of 10 deaths in a hurricane.

HURRICANE WARNING - Hurricane conditions are expected in the specified area of the Warning within 24 hours. Complete all storm preparations and evacuate dangerous or low-lying locations as soon as possible.

HURRICANE WATCH - Hurricane conditions are possible in the area of the Watch, usually within 36 hours. During a Hurricane Watch, prepare to take immediate action to protect your family and property in case a Hurricane Warning is issued.

STORM SURGE - A dome of sea water up to 20 feet high that arrives with a hurricane, and can affect as much as 100 miles of coastline. Evacuation zones are identified by their likelihood of being flooded by this rising water, which is responsible for most hurricane deaths.

TROPICAL DEPRESSION - An organized system of clouds and thunderstorms with a defined circulation and top winds of less than 39 mph.

TROPICAL STORM - An organized system of strong thunderstorms with a defined circulation and top winds of 39 to 74 mph. Tropical storms can quickly develop into hurricanes. Storms are named when they reach Tropical Storm strength.

TROPICAL STORM WARNING - Tropical storm conditions are expected in the specified area of the Warning within 24 hours.

TROPICAL STORM WATCH - Tropical storm conditions are possible within the specified area, usually within 36 hours.

TROPICAL WAVE OR DISTURBANCE - A cluster of clouds and/or thunderstorms without an organized circulation, moving through the tropics. Stronger systems start as Tropical Waves.

2. A WALK THROUGH A STORM:

Let's face it: Dealing with a hurricane is really a form of gambling. It's something most of us would rather not do, because usually there are more losers than there are winners. You will not know in advance whether a hurricane will strike in your locality or not, so the action you take to prepare for a hurricane may seem like it was a waste of effort after a near hit. However, if your community is struck by a hurricane and you have prepared properly, you and your family will have a better chance at winning. Being overly cautious and well prepared will result in a minimum of damage to property, inventory, and little or no injury to personnel.

If your location is within 200 miles of the coast, it’s very likely you'll have a chance to play at this game, like it or not. The good news is that there are a few rules you can count on.

a. TROPICAL STORMS:

Hurricane season begins in June and ends in November. During this period, you will begin to hear weather reports of tropical depressions and tropical storms forming hundreds of miles out in the Atlantic Ocean. Most of these storms wear themselves out before getting anywhere near land, but some don't. Each tropical storm is assigned a unique name which will follow it until it disperses.

b. HURRICANES:

If the highest sustained winds in the storm rise above 74 mph, the storm will be classified as a hurricane.

As a hurricane or tropical storm begins to threaten the U.S. mainland (typically 3 to 5 days before striking land), the National Weather Service will begin to issue a series of advisories on the storm. Each storm advisory includes a latitude, longitude, course, speed, mileage, and direction of the storm from the nearest major city. These advisories are issued at midnight, 6 a.m., noon, and 6 p.m. EDT, every day, as long as the storm remains a threat to the United States. Intermediate advisories may be issued as necessary to alert coastal interests to changes in the storm's path when landfall is imminent. You can hear the text of these advisories by 1) calling the nearest NOAA information recording, 2) listening to the weather broadcast on a VHF radio (162.550 MHz in Jacksonville, 162.400 or 162.475 in other cities), 3) or listening to the same broadcast repeated on cable TV channels (Channel 12 on Continental Cable in Jacksonville). Most TV and commercial radio stations will include the details of the latest hurricane advisory during their weather programs. Storm details are also published in local papers, but tend to be about 12 hours out of date.

You can watch the progress of a storm by plotting its coordinates from each advisory. You may want to post this chart near the entrance to your facility to remind your customers of the need to stock up on hurricane supplies. If a hurricane begins to threaten your locality, you should expect sales of hurricane supplies to increase. These will include: canned foods, flashlights and batteries, candles, bottled water, ice, matches, ready-to-eat foods, etc. (See Table 1 for a complete list). During this same period, it may be prudent to let your inventory levels of perishable items to drop lower than normal.

c. HURRICANE WATCH:

If the storm looks like it will strike land within the next 36 hours, a *Hurricane Watch* will be issued by the National Weather Service for the affected areas. At this point in time, it will be appropriate for you to meet with all of your employees and let them know what will be expected in the event of a landfall in your locality. You will also want to identify, at this time, those associates who may be unable to help during this period. Those associates living between the intracoastal waterway and the ocean, those living in house trailers, single parents with children or elderly relatives at home may all have to be dismissed before their co-workers.

d. HURRICANE WARNING:

If it appears that the storm is likely to strike your locality, a *Hurricane Warning* will be issued for your area. These warning are issued no more than 24 hours of the expected landfall, but the course of the hurricane is erratic, the warning may come only a few hours before landfall. Since hurricanes most often strike land in the early morning hours, a typical hurricane warning will be issued during the morning of the day before landfall.

During the day before, you can expect heavy sales. Many businesses will be closing early to give their employees time to prepare for the storm. It is very likely that the American Red Cross and Civil Defense Authorities will be announcing the opening of emergency shelters in your area, and some citizens will begin evacuation to shelters. This is the point in time when you should tape or board the windows of your location and begin to bring inventory indoors.

e. EVACUATION ORDERS:

Local government may recommend evacuation of specific areas along the coast. Evacuation orders should be taken seriously. The storm surge associated with a hurricane can cause water levels to rise 10 to 20 feet above normal along a wide stretch of coastline. Heavy flooding at the beaches is almost a certainty if the landfall is within 150 miles.

If your facility is in an evacuation zone, you should close as soon as possible after the announcement. If your associates live in an evacuation zone, they should be released immediately.

If your facility is not in an evacuation zone, business will continue to be brisk until the public perceives the danger to be too great to venture out. This may mean that you'll want to extend your hours beyond normal closing time, or you may want to close early. Your customers will be your guide here. You may also be forced to close early due to a power failure.

Since a power failure is very likely, you will want to take special precautions after closing. As many perishable foods (except produce) as possible should be stored in the appropriate freezer or cooler. Gas should be cut off prior to departure, and circuit breakers for all compressors should be turned off if the power has already failed.

Inventory near the front windows should be moved to a safe location in case of glass breakage and to avoid theft. One or two management personnel should be designated to remain in the facility after closing, provided evacuation has not been recommended. It will be their responsibility to activate all of the necessary precautions in the event of a power failure, and to protect the facility from looting.

f. POWER FAILURE:

As the winds pick up, power lines may be knocked down by falling trees causing a power failure. In this event, an order for dry ice should be placed as soon as possible if deemed as needed. The circuit breakers on all electrical equipment, appliances, coolers, freezers, and air conditioners should be turned off until after the power is restored.

g. LANDFALL:

The storm will either strike land in your vicinity, or will continue up the coast. Once a hurricane has passed, there is little chance of it returning to your location. If it passes, it will be safe to open for business as soon as the all-clear signal is

issued by the Civil Defense or the hurricane warnings for your area are lifted by the National Weather Service.

Because of this, all able employees should report to the location immediately after the storm to assess the situation, damages, and ready the location for business.

If the eye of the storm passes over your location, you may expect winds of 75 to 150 mph. If it passes within 150 miles of your location, you will still experience destructive winds. If it passes within 300 miles, you may expect gale force winds, exceeding 32 mph. Additional damage may also be caused by tornadoes spawned by the hurricane and inland flooding associated with the torrential rains or storm surge. Storms passing further than 300 miles usually produce only extended rain and tides slightly above normal.

If the storm strikes land in your vicinity, or passes just off shore, the range of possible destruction is dramatic: There may be no damage to your building and it's contents, or there may be no building left! You may never suffer interruption to electric power, or it may be out for as long as two weeks.

Ironically, your location may have been spared, but fallen trees, downed electrical lines, or heavy flooding may prevent your customers from shopping for several days. Flooding also may have deposited several thousand pounds of mud in your business.

TORNADOES:

Tornadoes generally occur during spring and summer, but can happen anytime during the year. With winds swirling at 200 miles an hour or more, a tornado can destroy just about anything in its path.

TORNADO WATCH: means a tornado is possible in your area.

TORNADO WARNING: means a tornado has been sighted and may be headed for your area. Go to safety immediately.

Follow these precautions:

- Pick a safe place where personnel could gather during a tornado. Make sure there are no windows or glass doors in the area.
- Turn off all utilities (electric, telephone, gas, etc...) prior to the storms arrival.
- Listen to local radio and TV stations for updated storm information.

After the tornado:

- Watch out for fallen power lines and stay out of the damaged area.

EVACUATION:

Local government may recommend evacuation of specific areas along the coast. Evacuation orders should be taken seriously. If your facility is in an evacuation zone, you should close as soon as possible after the announcement. If your associates live in an evacuation zone, they should be released immediately.

If your facility is not in an evacuation zone, business will continue to be brisk until the public perceives the danger to be too great to venture out. This may mean that you'll want to extend your hours beyond normal closing time, or you may want to close early. Your customers will be your guide here. You may also be forced to close early due to a power failure.

Since a power failure is very likely, you will want to take special precautions after closing. As many perishable foods (except produce) as possible should be stored in the appropriate freezer or cooler.

Gas should be cut off prior to departure, and circuit breakers for all compressors should be turned off if the power has already failed.

Inventory near the front windows should be moved to a safe location in case of glass breakage and to avoid theft. One or two management personnel should be designated to remain in the facility after closing, provided evacuation has not been recommended. It will be their responsibility to activate all of the necessary precautions in the event of a power failure, and to protect the business from looting.

POWER FAILURE:

As the winds pick up, power lines may be knocked down by falling trees causing a power failure. In this event, an order for dry ice should be placed as soon as possible if deemed as needed. The circuit breakers on all electrical equipment, appliances, coolers, freezers, and air conditioners should be turned off until after the power is restored.

SEVERE THUNDER STORMS:

Thunderstorms are always accompanied by lightning. These are intense local storms averaging 20 miles across and reaching as high as 10 miles.

When a storm approaches:

- Find shelter in a car or building.
- Unplug appliances and electrical/electronic equipment.
- Avoid using telephones or electrical appliances.
- Avoid taking a bath or shower, or running water for any other purpose. Metal pipes can conduct electricity.
- Turn off air conditioners. Power surges from lightning can overload compressors. This can result in costly repairs.
- Draw blinds and shades over windows. If windows break due to flying objects, the shades will prevent glass from shattering into your business.

If someone is struck by lightning:

- People struck by lightning carry no electrical charge and can be handled safely.
- Call for help. Dial 9-1-1 or your local Emergency Medical Services (EMS) number.
- Give first aid. If breathing has stopped, begin rescue breathing. If the heart has stopped beating, a trained person should give CPR.

EVACUATION:

Local government may recommend evacuation of specific areas along the coast. Evacuation orders should be taken seriously. If your facility is in an evacuation zone, you should close as soon as possible after the announcement. If your associates live in an evacuation zone, they should be released immediately.

If your facility is not in an evacuation zone, business will continue to be brisk until the public perceives the danger to be too great to venture out. This may mean that you'll want to extend your hours beyond normal closing time, or you may want to

close early. Your customers will be your guide here. You may also be forced to close early due to a power failure.

Since a power failure is very likely, you will want to take special precautions after closing. As many perishable foods (except produce) as possible should be stored in the appropriate freezer or cooler. Gas should be cut off prior to departure, and circuit breakers for all compressors should be turned off if the power is already failed.

Inventory near the front windows should be moved to a safe location in case of glass breakage and to avoid theft. One or two management personnel should be designated to remain in the facility after closing, provided evacuation has not been recommended. It will be their responsibility to activate all of the necessary precautions in the event of a power failure, and to protect the facility from looting.

VIII. DISASTER RECOVERY REFERENCE MATERIALS GLOSSARY OF TERMS

DISASTER PLANNING/RECOVERY REFERENCE MATERIAL

Bulgawicz, Susan L., CRM and Dr. Charles E. Nolan, CRM, Disaster Prevention and Recovery: A Planned Approach. ARMA International Publication Sales, 4200 Sommerset, Suite 215, Prairie Village, KS, 66208, 1988, ISBN 0-933887-28-0, 800-422-2762

The Disaster Recovery Journal. Disaster Recovery Institute, 2712 Meramer Drive, St. Louis, Missouri, 63129

Eulenbert, Julia Neibuhr. Handbook for the Recovery of Water Damaged Business Records. ARMA International Publication Sales, 4200 Sommerset, Suite 215, Prairie Village, KS, 66208, ISBN 0-933887-17-52, 1986, 800-422-2762.

ARMA International Standard Committee, Guideline - Magnetic Diskette Recovery Procedures. Prairie Village, KS: ARMA International Standard Committee, 1988.

BMS Catastrophe, Inc. Electronic & Magnetic Media Recovery. Special Technologies Division, 303 Arthur, Fort Worth, TX, 76107, 800-433-2940.

Association of Commercial Warehouse facilitys. Disaster Planning Workbook for Warehouse facilitys. ACRC Practices and Procedures Committee, 1990. ACRC, Post Office Box 20518, Raleigh, North Carolina, 27619, 919-821-0757.

Salvage of Water Damaged Books, Documents, Micrographic and Magnetic Media. Document Reprocessors of San Francisco, 41 Sutter Street, Suite 1120, San Francisco, California, 94104, 415-362-1290.

Vital Records Guidelines. ARMA International Standards Subcommittee, 4200 Sommerset, Suite 215, Prairie Village, KS, 66208, 1984/1991, ISBN 0-933887-14-0, 800-422-2762.

The Records & Retrieval Report. "Disaster Contingency Planning". September, 1992, Volume 8/Number 7. H. Wayne Gardner and Brett Balon. Greenwood Publishing Group, Inc. 88 Post Road West, Post Office Box 5007, Westport, CT, 06881, 203-226-3571.

DISASTER RECOVERY GLOSSARY OF TERMS

GLOSSARY OF TERMS

The following is a listing of the terms, and their definitions we use, in Disaster Contingency and Business Continuation Planning. Some of these terms are defined differently elsewhere; we might use them in a more narrow, or in a broader context, but in all cases we use these definitions in an attempt to clearly and concisely describe comprehensive disaster contingency and business continuation planning.

Accessibility (of information and data) - To be able to get at, or obtain, your information or product, when and where you need to. (See Availability; Useability)

Accessibility (of building, facilities, equipment) - To be able to enter your building or site, and your offices and facilities therein.

'After' phase (of a disaster) - The period during which repair, restoration and restitution takes place, as a part of restoring as-intended functioning. (See 'Before'; 'During')

Alternate site - A pre-planned work place, provided with appropriate facilities, equipment, information, data, and supplies, where staff can carry-out vital functions during the period in which the regular work site is inaccessible or unusable. Provisions are usually pre-arranged for transport of staff to the alternate site, and for catering and lodging while working there.

As-intended functioning. - The usual or normal day-to-day operations of the business in the course of providing its products or services. 'As-intended functioning' does not imply either the best manner in which the activities can be performed, or that the performance is stress-less; the meaning is that of 'the way things should go'.

Asset documentation - Recording, by photographic, video, or descriptive means, of the organization's physical property, equipment and furnishing, their location, and value. Such information is invaluable in substantiating insurance claims in the event of damage or loss.

Authentication procedures - Pre-planned verification steps to assure that only authorized personnel are activating the alternate site, declaring a disaster, moving operations to the alternate site, ordering building evacuation, and like emergency steps. These procedures are usually incorporated in specific, restricted-access copies of the Plan Manual.

Availability (of information and data) - That vital business information and data needed to provide products and services has been recorded and replicated for use wherever and whenever it might be required. (See Accessibility; Usability)

Avoidance - Planning and activities to prevent the things you don't want to happen from occurring.

Back-up (of information or data) - **v.** The process of creating one or more additional sets of information or data, on the same or different media, for use in the event that the initial information or data is not accessible or usable. **n.** The additional copies of information or data for use when out-of-course events, emergencies or disasters prevent access to, or use of, the initial data.

Back-up agreements - Agreements made with other organizations to enable your use of their building, infrastructure, facilities or equipment in the event that yours cannot be used, or vice versa. In considering back-up agreements, it is important to remember that many events that will disrupt your organization may also disrupt most of your neighborhood.

Back-up site - An alternate site.

'Before' phase (of a disaster) - That time period, before which an emergency, out-of-course event, or a disaster strikes your organization, when you have opportunity to create a disaster preparedness and business continuation plan. Your 'Before' phase may end as you read this! (See 'After'; 'During')

Building - The edifice which you own or in which you rent or lease space for staff to conduct business or manufacture products or provide services and/or to store material.

Business continuation - The functioning of your organization during the periods of emergency, out-of-course events, or disasters, and the return to as-intended functioning.

Business impact analysis - The determination of what affect any out-of-course event, emergency, or disaster will have upon the ability of the business to function or to perform its activities.

Business interruption - The stoppage of business functioning. No services are being provided; no products being produced; no support services being rendered.

Business recovery - Return to as-intended functioning. This encompasses restoration and restitution (q.v.) as well as return to operations in the original building(s) or in replacement building(s). It also includes financial reimbursement for loss or damage.

Capacity - A system's ability to handle the amount of information and/or product with which it is likely to be presented under the most adverse conditions. A vital factor in alternate site planning.

Cold site - An alternate site, associated with data processing. Usually only a building and infrastructure lacking any equipment, facilities, information, data, supplies or other provision for staff.

Communications security - (1) Safe-guarding of information or data during its transmission because of the confidential or sensitive nature of the information of data. (2) Steps taken to assure the integrity of a communications systems, or to reduce the vulnerability of the communications system to emergencies, out-of-course events, or disasters. Alternate communications systems, or redundancy, is frequently utilized.

Contingency - The planned or programmed response to an event; the availability of an alternate means or method.

Critical functions - The functions or activities within a business that must necessarily be accomplished. Critical functions (and their antithesis, "nice functions') are usually time-line based. Payroll preparation may not be a critical function on Monday, but it may be on Thursday! Maintenance of mailing lists may not be critical in the short-term, but after ten days, it might be

vital to up-date them. Critical functions, and when functions become critical, is one of the initial determinations in creating a disaster contingency and business continuation plan.

Critical data; critical information - That data and information that must be in hand in order for the critical functions to be performed.

Damage mitigation - The process of stemming or preventing damage to building, infrastructure, equipment, facilities, furnishing, and other contents that might result from an emergency, out-of-course event, or a disaster. Pre-planning, as a part of disaster contingency and business continuation planning, establishes resources to mitigate any damage, as well as to provide information on what should be saved first, where it is located, and how it should be saved.

Data - That part of an organization's information that is recorded, stored, or processed utilizing magnetic or optical media. (See Information)

Data protection - Practices and procedures to assure that data is available, accessible, and usable, whenever and wherever needed.

Disaster - The consequence of an emergency or out-of-course event, when normal or as-intended functioning or performance is impossible or impractical. Preparedness planning, alternate site(s), and back-up prevent an emergency or out-of-course event from escalating into a disaster. In many definitions, 'disasters' are direct events; we consider 'disasters' the results of failure to properly establish contingency plans. As an example, a severe storm is not a disaster; failure to plan for continued operations in spite of the storm can result in events escalating into a disaster wherein your organization cannot function or perform. (See Emergency; Out-of-course event)

Disaster contingency planning - The science and art of creating a plan that will enable an organization to cope with and survive out-of-course events, emergencies and disasters.

Disaster management center - The pre-planned location, within the organization's building if such is usable, or at a pre-planned site from which the emergency or out-of-course event is managed and responses directed.

Disaster management team - Key members of the organization's staff who evaluate the circumstances of the emergency or out-of-course event, its potential length, and the requirements necessary to continue operations and to prevent the occurrence from escalating into a disaster. This management team, in conjunction with the Alternate Site management team, initiates alternate site operations. Duties, responsibilities, and authority of the disaster Management team, and its alternate members, are iterated in the Plan Manual. The Disaster Management team should also include a coordinator from pre-selected specialists in damage mitigation and restoration.

Disruption - Any event negatively impacting a function of the organization.

Drill - A practice session, emulating an emergency or out-of-course event, intended to provide fine-tuning of in-place procedures, and to assure that individual systems and procedures are proved, that all systems and procedures can work together, and to prove that the disaster contingency plan is able to deal with normal and emergency conditions.

'During' phase (of a disaster) - The period during which the as-intended function of the organization is interrupted or halted. In this phase, contingency plans are activated, and the disaster management team superintends over all activities. (See 'After'; 'Before')

Dynamic information - Information frequently used and information subject to on-going change.

Emergency - An occurrence, such as a work stoppage, storm warning or an evacuation because of potential danger, that does not physically impact as-intended function, but does impair, impede, interrupt or cause the halt of as-intended functioning. (See Out-of-course event)

Equipment - The 'hardware' an organization uses, including computers, word processors, copiers, fax machines, telecommunications equipment, office mechanicals, desks, chairs, and like furnishings necessary for the organization to perform its functions.

External (causes) - Those out-of-course events and emergencies that occur outside of the organization but have direct impact on its functioning. External causes or events include Natural,

Human-intervention, Technologic, and Infrastructure occurrences. (Refer to each of these latter definitions.)

Facilities - The space an organization occupies within a building or site, including reception areas, lobbies, offices, conference rooms, libraries, cafeterias, warehousing areas, and the like, wherein and wherefrom an organization functions. 'Facilities' can also include lounges, exercise rooms, and the like.

Failure - When an expert of the building, infrastructure, equipment, facilities, or computer software does not work, or staff cannot work. (See Fault)

Failure probabilities - The statistical (or other) likelihood that a specific failure will occur. This serves as a guide in planning and allocation of resources. (See Risk)

Fault - When an aspect of the building, infrastructure, equipment, facilities, or computer software does not work as intended, or the staff cannot work as intended or normally. (See Failure)

Fault correction sequence - The pre-determined sequence in which specific faults are to be corrected. The sequence is designed to preclude additional faults or failures, minimize fault duration, and minimize the duration in which as-intended functioning is impacted, impaired, impeded, interrupted or halted.

Hot site - An alternate site wherein resources and equipment for contingency functioning are located. The type and amount of equipment and other resources vary, from scant ability to continue some operations to complete resources necessary to carry on deemed business functions.

Human error - A mistake, misapprehension, misunderstanding, misjudgment; a blunder, slip or oversight in a person's actions.

Human error consequence - The result of a human error on the as-intended function of an organization.

Human intervention events - An event that is caused by a person or persons that impacts the as-intended functioning of the organization. The person or persons can be employees or staff members ('Internal') or others ('External'). Human intervention events include sabotage, vandalism, strikes, mischief, kidnapping, arson, and purposeful omissions.

Impair - To diminish the value, excellence or integrity of an activity or function.

Impede - To slow, obstruct or hinder the functioning or accomplishing of a task or activity.

Information - The 'facts and figures' of a business that a business requires to produce its products or to provide its services. Recorded information can be on hard copy, usually paper and eye-readable, microfilm or microfiche. (Information recorded on magnetic or optical media is considered 'data', q.v.)

Information security - Practices and procedures to assure that information will be available, accessible, and usable, whenever and wherever needed.

Infrastructure - Those elements of a building or site that are 'permanent', such as elevators, heating, ventilating, and air conditioning systems, power systems, and piping for water supply and waste water disposal.

Insurance audit - A professional assessment of an organization's insurance coverage for its building, infrastructure, facilities, equipment, staff, and business continuity to determine (1)

whether or not coverage has been provided for faults and failures that management believes and wants coverage; (2) whether or not the provided coverage is in amounts that management believes is adequate; and (3) that the organization's day-to-day functions are in compliance with the provisions and restrictions of the coverage, so that if a loss occurs, proper restitution will be made by the insurance carrier.

Internal (causes) - Those out-of-course events and emergencies that occur within the organization, and have direct impact on the as-intended functioning and activities. Internal causes include Human-intervention, Technologic, and Infrastructure occurrences. (Refer to each of these latter definitions.)

Interruption - A halting or stoppage, for a relatively short period, of the as-intended functioning or activity.

Loss - When a building or part of a building, or part or all of its infrastructure, facilities, equipment or furnishings are damaged, destroyed or rendered useless.

Manual - See Plan Manual.

Material - The aggregate or things (e.g., equipment, supplies, facilities) used or needed in any business or undertaking (as distinguished from personnel). Not to be confused with material.

Natural events - Any event, 'caused by Nature' or by "act of God' that impacts the as-intended functioning of the organization. Natural events include storms, lightning, earthquakes, flood, hurricanes, and magnetic storms.

Out-of-course event - Any event not a part of planned for operations that impacts the as-intended functioning of the organization. This can be caused by natural, technologic or human-intervention events and can lead to a disaster if not addressed properly.

Plan Manual - The codification of an organization's disaster preparedness and business continuation plan. A Plan Manual contains the logistics, systems and procedures for implementation of the Plan, and provides guidance and procedures to be followed in preparation for, and during the time span when operations are impeded, impaired, interrupted or halted due to events that are not a part of normal business functioning. The Plan Manual also serves as a reference for all members of the organization, and iterates procedures and action steps that are necessary to reduce present and potential vulnerabilities, in, and risks to, the organization's building, infrastructure, facilities, equipment, information, data, and staff. The Plan Manual is the reference in which is set forth the strategies and logistics, and procedures and action steps, necessary for the organization's business continuation and survival when an emergency, out-of-course event, or a disaster strikes. We also refer to this as the 'Primer for Survival'.

Recovery - The process or time period in which material and operations are being restored to a state of as-intended functioning.

Recovery site - An alternate site (q.v.) used when the regular work site, or its contents, are inaccessible or unusable. The term, 'alternate site' is much preferred.

Rectification - The process of correcting faults and failures so that as-intended performance or functioning will be achieved.

Remedial steps - The individual steps or actions taken in correcting faults and failures, or in reducing or eliminating vulnerabilities.

Restitution - Payment by insurance companies in compensation for losses incurred. (See Insurance audit)

Restoration - The process - including cleaning, repairing, drying, de-odorizing, painting, and refinishing - of returning material to its condition prior to a loss.

Risk - The relative probability or chance that a particular fault or failure will occur, or that a particular Natural, Human-intervention, Technologic, or Infrastructure event will occur. The relative vulnerability to an out-of-course event, emergency or disaster. (See Failure probabilities)

Security - The physical protection afforded the site, building and contents, to the staff working there, and to visitors, to assure their safety and well-being.

Sensitivity - (of information and data). The relative confidentiality of the organization's information and data, relative to business and trade secrets. The greater the sensitivity of the information, the greater the amount of protection it must be afforded to assure against theft, compromise, or unauthorized access or use.

Technologic events - Any occurrence caused by, or related to, the use of technology, that impacts, impairs, or impedes the as-intended functioning of the organization. Technologic events include the shortage or failure in supply of electricity, common carrier telecommunications, computer and software failures, local- and wide-area computer network failures, electro-magnetic interference and electro-magnetic radiation.

Test - A practice session. A period of adjustment and demonstration that all systems can work together as intended.

Transparently - The ability to conduct activities and functions under other than as-intended conditions without customer or client awareness that you are operating, say, from your alternate site.

Triage - The decision process, by the Disaster Management Team (q.v.), in determining what requirements are necessary to preparedness plan should be activated to assure business continuity.

UPS - Uninterruptible Power Supply. A back-up power supply, usually battery-based, that furnishes sufficient and correct power to (1) allow safe and orderly shut-down of computing facilities without loss of data or damage to the equipment; or (2) to allow emergency functioning of telephone or other telecommunications equipment; or (3) to provide emergency lighting or elevator power; or (4) to provide a continuity of emergency power until an emergency or stand-by generator is activated and functioning. The term UPS is frequently used to describe a device intended only to filter out undesirable fluctuations in the main power supply.

Usability - (of information and data). Information or data must be able to be read and comprehended to be of any value. Codes, explanations and keys must be available for eye-readable information; hardware and software, and computer codes need be available for magnetic media; indexes and locator aids for stored microform and paper records. (See Accessibility; Availability.)

Vulnerability - An area of function that may be impacted by a Natural, Human-intervention, Technologic or Infrastructure event, resulting in an impaired, impeded, interrupted or halted as-intended functioning or activity. An organization's building, information, data, and staff are each vulnerable to out-of-course occurrences and emergencies caused by Natural, Human-intervention, Technologic, and Infrastructure events. Such vulnerabilities, and the consequential impact, can be reduced, minimized, or eliminated in a disaster contingency program.

Warm Site - A partially equipped (hence, partially prepared and ready) alternate or back-up site. Less ready than a Hot Site (q.v.) yet more ready than a Cold Site (q.v.) - ('Cool'' and 'Tepid' site probably exist, too!)

All American Records Management (AARM)

PRIVACY AND SECURITY POLICY

ESTABLISHED INTERNAL SECURITY CONTROLS DESIGNED TO PROTECT AARM INFORMATION, WHILE SAFEGUARDING THE PRIVACY AND UNAUTHORIZED USE, OR DISPOSAL OF CLIENT RECORDS AND DATA

Privacy and Security Policy

TABLE OF CONTENTS

Privacy and Security Policy

INTRODUCTION

AARM has developed the following controls to safeguard information from unauthorized use, disposal, disclosure, damage or loss:

Administrative Safeguards **Section I**

Documented policies and procedures for day-to-day operations; managing the conduct of employees with records and information management; and managing the selection, development, and use of security controls.

Physical Safeguards **Section II**

Security measures meant to protect an organization's information systems, as well as related buildings and equipment, from natural hazards, environmental hazards, and unauthorized intrusion.

Technical Safeguards **Section III**

Security measures that specify how to use technology to protect records and information management, particularly controlling access.

Privacy and Security Policy

PRIVACY & SECURITY RESPONSE TEAM

Should you have any questions regarding this written Privacy and Security Policy, or should you wish to inquire about or report a possible violation, emergency or any unauthorized breach of confidential data, please contact the following:

Security and Privacy Response Team

Mr. Grant R. Eckhardt, President — ***Records Center***
AARM Records Management
15580 E. Hinsdale Circle
Centennial, CO 80112
Phone: 303-373-5101
Email: geckhardt@aamsmoves.net

Mr. Joe Slinger, Operations Manager — ***Records Center***
AARM Records Management
15580 E. Hinsdale Circle
Centennial, CO 80112
Phone: 303-373-5101
Email: jsager@aamsmoves.net

Mr. Rob Bosch — ***IT/Network Assistance***
IPremise
9085 E. Mineral Circle, Suite 195
Centennial, CO
Phone: 303-242-5040
Email: rbosch@ipremise.net

Mrs. Diane Hyman — ***Records Software***
DHS Worldwide, Inc.
563 Blanding Boulevard, Suite 3
Orange Park, Florida 32073
Phone: 800-377-8406
Email: admin@dhsworldwide.com

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

EMPLOYEE IDENTIFICATION AND ACCESS

Provision of Identification Badges

- An Identification Card Request Form will be completed and maintained on each employee.
- New employees will complete their portion of the Identification Card Form and Confidentiality Agreement during the first week of employment. A temporary ID badge will be issued.
- The supervisor will transmit the Identification Card Form to the General Manager, who will then approve and transmit it for processing.
- Upon receipt of the Identification Card Form, the General Manager will schedule the time the employee is to be digitally photographed. The completed ID badge will then be provided to the employee as a replacement for the temporary id badge.

Lost Identification Badges

- An employee who returns a damaged identification badge to their supervisor will be issued a replacement badge at no cost not to exceed one identification badge per calendar year.
- An employee who loses the identification badge shall report the loss to his or her supervisor within one workday.
- The office will replace one lost identification badge per employee per calendar year.
- Employees will be charged the cost of replacing a lost identification badge after the first one annually.
- The Security Officer shall be responsible for deactivating lost cards.

Separation of Employment

- The supervisor shall obtain the identification badge and any AARM issued keys from every employee during the last week of employment.
- The supervisor shall then present the identification badge and issued keys to the General Managers by the employee's last workday before separation. The Security Officer shall deactivate the card.

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

EMPLOYEE IDENTIFICATION AND ACCESS

Building Security Procedures

- All employees shall openly wear their identification badge so that it is visible at all times while within the building.
- Don't let someone you don't know follow you in the building before and after normal business hours.
- If you see someone outside your building who is waiting to get in, direct him/her to the designated entrance to the building where security personnel or receptionist are located.
- All visitors shall sign in, complete a confidentiality agreement, and be issued a visitor's badge to wear for the duration of the visit. Visitors must surrender their driver's license which will be returned upon receipt of their issued visitors pass.
- Each employee is responsible for observing and notifying a person without an identifying badge, guiding the person to the security desk in the lobby to receive a badge or reporting the person's presence to their supervisor at once.
- All employees and visitors shall enter and exit the building from the front doors; all other doors are emergency exits.
- Report any suspicious activity to your supervisor, and/or the General Manager.

Level of Card-Access

The General Manager and the Security Officer are jointly responsible for determination of levels of card access based on: 1) Safety and Liability of the buildings, and 2) the nature of work of employees occupying the buildings. Only an employee assigned to the record and data center as his or her duty station may request card-access.

- No Access - The card will not open the door to the buildings.
- Daytime Access - 6:30 A.M. to 6:30 P.M., Monday through Friday.
- Extended Day Access - 6:30 A.M. to 10:00 P.M., Monday through Friday
- Extended Week Access - 6:30 A.M. to 6:30 P.M., Monday through Saturday.
- Extended Day/Week Access - 6:30 A.M. to 10:00 P.M., Monday through Sunday.
- Unlimited Access - 24 Hours a day, seven (7) days a week.

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

EMPLOYEE IDENTIFICATION AND ACCESS

Change in Access Status

Any change of access status for an employee must be approved in writing by both the General Manager and Security Officer and must include the information shown below.

The employee's name and title, the current access level, the desired access level, and reason(s) for the change.

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

EMPLOYEE CONFIDENTIALITY AGREEMENT

Confidentiality Agreement

This agreement is effective _____between _____ the AARM and _____, the Employee.

AARM employs the employee to perform professional services usually and normally incident to the business of records storage and retrieval services. The employee and AARM recognize that sensitive information of the AARM's clients is store and managed at AARM facilities. The employee agrees to protect this information regarding the location of or the information stored at any of AARM's facilities.

In addition, the employee recognizes that the list of AARM customers and the rate schedules that apply to these customers are a valuable, special and unique asset of AARM business. The employee will not, during or after the term of his/her employment, directly or indirectly disclose the list of AARM customers, or any part thereof, or any rate information to any person, AARM, corporation, association or any other entity whatsoever. The employee acknowledges that during his/her employment he/she will become familiar with trade secrets, competitive information or confidential information of AARM, and the employee will not, during or after the term of this agreement, disclose any of such valuable information.

In the event of an actual or threatened breach of confidentiality by the employee, AARM shall be entitled to an injunction restraining the employee. If a lawsuit is necessary to enforce this agreement, the employee agrees to pay all legal expense and attorney's fees including court costs.

Witnesses:	**AARM:**
_____	_____
Date: _____	Date: _____
Witnesses:	**Employee:**
_____	_____
Date:_____	Date:_____

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

EMPLOYEE ETHICS POLICY

Overview

The purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

We are committed to protecting employees, customers, partners, vendors and AARM from illegal or damaging actions by individuals, either knowingly or unknowingly. AARM addresses issues proactively and uses correct judgment, which we believe sets us apart from competitors.

AARM will not tolerate any wrongdoing or impropriety at anytime. We will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

Purpose

Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties.

Policy

Executive Commitment to Ethics

1. Management must set a prime example. In any business practice, honesty and integrity must be top priority for executives.
2. Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.
3. Executives must disclose any conflict of interests regard their position within AARM.

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

EMPLOYEE ETHICS POLICY

Employee Commitment to Ethics

1. AARM employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
2. Every employee needs to apply effort and intelligence in maintaining ethics value.
3. Employees must disclose any conflict of interests regard their position within AARM.
4. Employees will help AARM to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

AARM Awareness

- Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
- AARM will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within AARM.

Maintaining Ethical Practices

- AARM will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.
- Employees should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
- AARM has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

Unethical Behavior

- AARM will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
- AARM will not tolerate harassment or discrimination.
- Unauthorized use of AARM trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of AARM will not be tolerated.
- AARM will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.
- Employees will not use corporate assets or business relationships for personal use or gain.

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

EMPLOYEE ETHICS POLICY

Enforcement

- Any infractions of this code of ethics will not be tolerated and management will act quickly in correcting the issue if the ethical code is broken.
- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

DRIVER HIRING PRACTICES

General

- Driver/couriers are considered to be one of the most important customer service representatives because of their personal contact with local as well as national account customers. Good driving record required. Courier must be well groomed and practice good personal hygiene.

- Pickup/deliver records at multiple customer sites. Being mindful of the time sensitive nature of deliveries, ensure that all work requests are transported by deadlines set. Due to regulations and legal requirements, the safety and security of records must be maintained at all times with no records left in an unattended, unlocked vehicle or building holding area. Ensure records are delivered to authorized requestors. Magnetic media should be maintained in climate controlled environment at all times.

- This position requires that from time to time the employee may be called upon to respond to emergency pager for deliveries after hours, weekends and holidays.

- Perform out-of-city pickups/deliveries and also Saturday/Sunday pickups/deliveries if scheduled (as needed)

- Courier is responsible for general maintenance of AARM vehicles – fuel, tire pressure, battery, water levels, and fire extinguishers (if required). At end of day, all records to be offloaded to pallets at warehouse and vehicle cleaned of any debris. Report to supervisor immediately any perceived or real mechanical problems with AARM vehicles. Complete vehicle logs if required.

- Driver must be versed in using cellular phone and adhere to establish procedures and practices which will increase communication and productivity between driver and operations.

- Driver should receive training on properly handling documentation on inbound/outbound orders. Signatures should be secured on all documentation. Security pouches should be used on all documents/files transported.

- Customer courtesy procedures are important to be reviewed with drivers. Being polite and courteous should be the priority during each customer interaction.

- Driver is responsible for reporting any accident to a supervisor immediately. Any damage to customer facility should be reported to property management and immediate supervisor before leaving customer site.

- Each driver is issued picture identification card, which must be worn on the outside of the uniform at all times

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

DRIVER HIRING PRACTICES

Driver Qualifications

- Each driver candidate must possess valid driver's license with chauffeur endorsement. State may require CDL (commercial driver's license) with appropriate class identified, depending on truck weight and size).
- Each candidate must possess a satisfactory Motor Vehicle Report (MVR), with annual review of driving record.
- Each driver must submit to annual physical examination.
- Each candidate must submit to, and produce a negative result from, a drug screen urinalysis.
- Each driver must pass AARM qualification procedure including successfully completing a road test.
- All insurance AARM requirements must be met.

Privacy and Security Policy

SECTION I – – ADMINISTRATIVE SAFEGUARDS

STAFF HIRING PRACTICES

General Staff

Security starts with hiring the right people. AARM strives to reduce personnel risks by taking steps such as checking references, performing background investigations and drug screening program.

Accounting personnel are required to provide financial information for additional security checks.

Any temporary staffing will be checked through temporary staffing agency for suitability. Must meet agency standard hiring criteria.

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

SAFETY AND SECURITY

Facility Access Procedures – Visitors

Protection from unauthorized access is a required feature for our record center. All visitors, clients, prospects, and vendors, must be required to sign into the visitors facility log, wear an assigned visible ID badge, and sign a confidentiality agreement.

VISITORS CONFIDENTIALITY AGREEMENT

This confidentiality agreement ("Agreement") is entered into by and between _____("The Center") and _____(Visitor). The visitor must have full authorization to act as a legally binding signatory or must obtain a legally binding and authorized signature prior to attendance at the Center. The party representative for disclosing or receiving is_____ (Visitor/AARM).

The Visitor agrees that: The Visitor accepts that the Center stores Confidential Information at its facility that it is protected as provided by this Agreement.
The term "Confidential Information" under this Agreement means information that may be disclosed or by the Center to the Visitor or that may be observed by the Visitor while in this facility. Confidential Information includes customer identification, security procedures, and rates, services, and contract information.
This Agreement relates to the disclosure of information made during the period commencing on the arrival date and time of the Visitor and expiring on their date and time of departure.
The Visitor may not disclose the Confidential Information to any person except its employees, consultants, and subcontractors to whom it is necessary to disclose the information for discussion or evaluation.
The Visitor's duties under this Agreement shall apply to any information provided orally, visually or in any written document, or other material developed or prepared by the Center.
Confidential Information shall not include any item of Confidential Information which: (a) is within the public domain prior to the time of the disclosure by the Visitor to the Center or thereafter becomes within the public domain other than as a result of disclosure by the Visitor or by any of its representatives in violation of this Agreement; (b) was, on or before the date of disclosure in the possession of the Visitor as evidenced by records.
This Agreement does not grant any License to Confidential Information.
This agreement shall be governed in accordance with the law of the state within which the Center resides.
The Visitor may not assign this Agreement or any interest herein without the Center's express prior written consent.

Signed for and on behalf of

Visitor/Authorized Signatory:

Name: _____ Title: _____

Signature: _____ Date: _____

Privacy and Security Policy

SECTION I - ADMINISTRATIVE SAFEGUARDS

SAFETY AND SECURITY

Facility Access Procedures – Clients

One of the many protection features offered by our record center is the restriction of unauthorized access to the client's records. Each client will be requested to provide a list of authorized users, with security pin numbers that identifies what level of access the user has. This level can be for all records, department records only, or individual box records.

When requesting services from the record center, the requestor must have their authorization code approved before the requested service can be performed. Existing record center software program automates this process.

Should the client call for picking up their own records at the records at the center, an security authorization procedure must be followed.

SECURITY REQUIREMENTS AND ACCESS PROCEDURES

Visitors must remain in lobby area and may not access secured areas unless escorted by a _____(Record Center) employee. Visitor ID badge must be displayed while at the facility.
No photographic equipment, briefcases or other containers will be allowed beyond the lobby area.
Persons receiving information for client at a _____(Record Center) must, upon checking in, present three (3) pieces of identification: 1) driver's license (with photo); 2) AARM identification, and 3) _____(Record Center's security code number).
Persons not in possession of _____(Record Center's security code number) must have a letter of introduction on Depositor's letterhead signed by an authorized representative.

Persons desiring access must be prepared to wait for telephone verification.
All data and items removed from secured area must be recorded and signed for by properly authorized depositor representative.
Persons making requests for information via telephone or in person must be on Authorization for Access form and will be required to give security code number.
Depositor is responsible for completion of _____(Record Center's Authorization for Access form.) Depositor is responsible for all additions to, and deletions from, Authorization for Access form.

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

COMPLIANCE STATEMENT

Compliance Statement

By providing the following safeguards, AARM maintains that the records center services and operations addresses the privacy and security of client information as described in the following legislative rules, as to unauthorized use, disclosure, disposal, damage or loss:

- Secure facility with intrusion and fire protection systems
- Employee Confidentiality Agreement
- Client Authorized User Form reviewed and submitted periodically
- Client Web Authorized User Form reviewed and submitted periodically
- Standard operating procedures regarding authorized record request
- Standard operating procedures for secure pickup and delivery
    - Secured vehicles
    - Authorized delivery signatures
    - File security pouches with numbered seals
- Standard operating procedures regarding written record removal requests
- Certified destruction (shredding) guidelines

1. ***Sarbanes-Oxley Act of 2002 (SOX)***

2. ***Gramm-Leach-Bliley Act (GLB), November 1999***

3. ***Fair and Accurate Credit Transactions Act of December 2003 (FACTA) and The FACT Act Disposal Rules***

4. ***Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA)***

5. ***Rules 26 & 34 of the Federal Rules of Civil Procedure (Record Hold)***

Discovery Notification - Record 'Hold' Guidelines

- Client Legal Department should communicate the hold notification in writing to the records center with detailed listing of records to be "held"
- Record center revises record series category for records listed and assigns permanent retention period
- Periodically "holds" should be reviewed and lifted as applicable.
- Updates to be issued by Client Legal Department for "hold" removal dates

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

CLIENT AUTHORIZATION FOR ACCESS FORM

Authorization for Access

To facilitate your requests and to keep our information current, please fill in as indicated and return this form to our office. The signatures of the persons authorized must appear opposite their names.

The form is sent to you in duplicate but we require the original only. Please keep the copy for your own files.

Thank you.

Access Authorization

This shall be considered authorization for the
Following named individuals to have access
To the contents held in the account of:

Account Name (optional)	Account number	Code
Porter Law FAARM	15444	1632
Printed Name	**Signature**	

Betty Johnson	xxxxxxxxxxxxxxxxx	1632-1
Beverly Smith	xxxxxxxxxxxxxxxxx	1632-2
Jack Baker	xxxxxxxxxxxxxxxxx	1632-3

Voids all Previous Authorizations ❑

Additions to previous Authorizations ❑

Approved by:	Position	Date
Gordon Turner	Purchasing Director	3/10/207

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

CLIENT WEB USER AUTHORIZATION FOR ACCESS FORM

Web User - Authorization for Access

To facilitate your requests and to keep our information current, please fill in as indicated and return this form to our office. The signatures of the persons authorized must appear opposite their names.

The form is sent to you in duplicate but we require the original only. Please keep the copy for your own files.

Thank you.

Access Authorization

This shall be considered authorization for the
Following named individuals to have access
To the contents held in the account of:

Account Name (optional)	Account number	Code
Porter Law FAARM	15444	1632
Printed Name	Signature	

	Authorized Privileges
Betty Johnson	Administrator
Jerry Jackson	Group 1
Janet Smith	Group 2
Elizabeth Stallings	Group 2
Michael Best	Group 3

Permissions Instructions

Administrator	Add users/delivery sites/all group 1/2/3 functions
Group 1	Add/inquire/request/remove/report
Group 2	Inquire/Request only
Group 3	Inquire only

Voids all Previous Authorizations ❑

Additions to previous Authorizations ❑

Approved by:	Position	Date
Jaclyn Burris	Senior Vice President	01/23/07

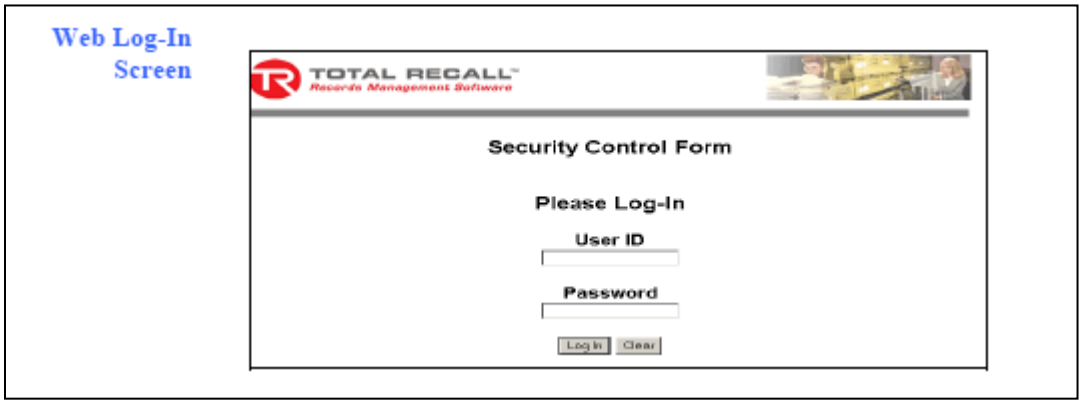
Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

CLIENT WEB USER AUTHORIZATION FOR ACCESS FORM

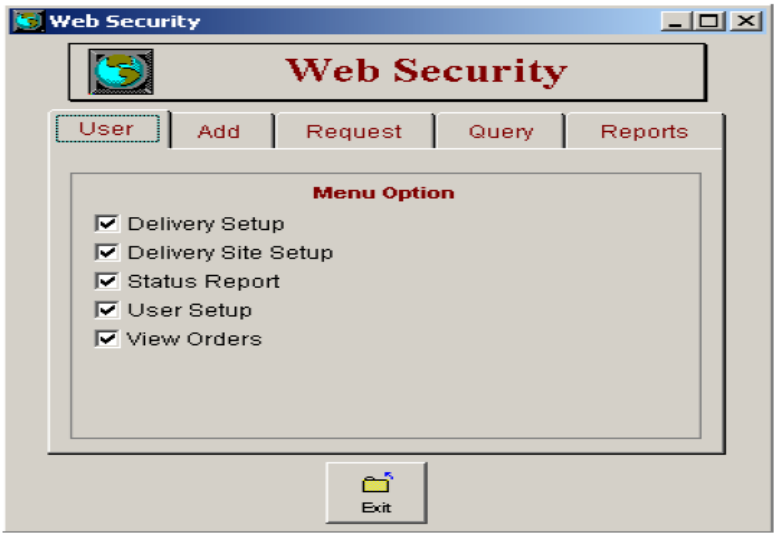
Unauthorized users, attempting to Log-In to the Web Module will receive the following message; “User ID or Password Invalid!”

Web Log-In Screen



As an additional security measure, a single Client “Administrator” should be established and allowed to have rights and permissions to setup other users and alternate delivery sites.

Web Security Button Screen



Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

RETRIEVAL/DELIVERY PROCEDURES

Record Retrieval/Delivery Procedures

Record Retrieval

- Client places retrieval request for carton/file through email, fax, phone or Web
- Verification of requestor made from authorized access list
- Work order created, printed and sent to warehouse for retrieval
- Item barcodes are scanned for quality purposes and item status updated on computer
- “File out” cards are placed into cartons to replace file retrieved
- File requests are placed in security pouches with tamper proof numbered seal affixed, or enclosed/envelopes/containers
- Large groups of files may be shrink-wrapped for added security

Record Delivery

- Items are placed on vehicle at secure facility dock door and vehicle door locked. At time of delivery to customer, items are checked off for quality assurance and loaded onto delivery equipment. Vehicle locked for security purposes while drive away
- Driver returns with customer proof of delivery signature. Any items picked up at same time are scanned to work order and placed staging location.

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

REMOVAL/DESTRUCTION PROCEDURES

Record Removal/Destruction Procedures

Permanent Removal – Containers are retrieved and returned to customer for their disposition

Destruction – Containers are retrieved and sent to third part vendor for destruction, per customer instructions. In-house destruction rules may apply.

Destruction review report created at records center for all containers to be reviewed for destruction for designated period. Review period established by customer at time container was originally added to inventory.

- Destruction report sent to customer for final removal authorization
- Client places retrieval request for carton/file through email, fax, phone or Web
- Verification of requestor made from authorized access list
- Work order created, printed and sent to warehouse for retrieval
- All cartons pulled for destruction should be verified again by the warehouse manager before release to the destruction service. Verification should be made against original destruction request—not work order
- Certificate of Destruction provided to customer

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

REMOVAL/DESTRUCTION PROCEDURES

Record Removal/Destruction Procedures – Sample Report

DATE: 04/29/2007
TIME: 17:00:47

DHS Worldwide
CONTAINER EXPIRATIONS - BY CUSTOMER AND EXPIRATION DATE
CUSTOMER: DIA001 Diane's Dress Shop
DATE RANGE: 01/01/2007 TO 04/30/2007

PAGE: 1
RTRP0700A

CUSTOMER BOX #	LOCATION TR CON #	STRG CODE	DESCRIPTION/	FROM/TO DATE	EXPIRE DATE	SERVICE CODE DESCRIPTION	ACTION SPECIFIED	INI
1004	1-01-A-01-04 15722	SR1	INVENTORIES - APRIL 2001		04/01/2007		_____	___
1003	1-03-A-01-03 15721	SR1	INVENTORIES - MARCH 2001		03/01/2007		_____	___
1001	1-03-A-01-06 15719	SR2	INVENTORIES - JAN 2001		01/15/2007		_____	___
1002	1-03-A-01-06 15720	SR2	INVENTORIES - FEB 2001		02/01/2007		_____	___

TOTAL CONTAINERS FOR CUSTOMER: 4
=======

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

CERTIFIED DESTRUCTION CERTIFICATE

Certificate of Destruction – Sample

DATE: 04/29/2007
TIME: 17:06:01

PAGE: 1
RTRP0700D

DHS WORLDWIDE
AUTHORITY FOR DESTRUCTION

ACCOUNT: DIA001 - DIANE'S DRESS SHOP
1772 UNIVERSITY BLVD. WEST
JACKSONVILLE, FL 32217

RECORDS TO BE DESTROYED

Container Number	Customer Box #	Description	Destruction Date Expire Date	Revised Date
15719	1001	INVENTORIES - JAN 2001	01/15/2007	_____
15720	1002	INVENTORIES - FEB 2001	02/01/2007	_____
15721	1003	INVENTORIES - MARCH 2001	03/01/2007	_____
15722	1004	INVENTORIES - APRIL 2001	04/01/2007	_____

AUTHORIZATION

Authorization is hereby given for the disposal of the records listed above.

_____ X_____ _____

Date Signature Title

CERTIFICATE OF DESTRUCTION

Date Destroyed:_____ Signature: _____

DHS WORLDWIDE Hereby certifies that on this date, the account's records listed above were destroyed. Items marked with a revised destruction date were not destroyed, and will remain in storage until the date specified.

Privacy and Security Policy

SECTION I – ADMINISTRATIVE SAFEGUARDS

RECORDS CENTER MANUALS

Various records center policies, procedures and manuals are available for review by client, upon request.

1. ***Standard Operating Procedures***
2. ***Client Policy and Procedures Manual***
3. ***Disaster Contingency Planning***
4. ***Work Flow Procedures***

Privacy and Security Policy

SECTION II – PHYSICAL SAFEGUARDS

SECURITY GUIDELINES

Stability, References

Customize information on following areas:

Financial stability
References from local businesses
Owned/leased facilities
Expansion capabilities
Technology investment
Community activities
Years of service (parent company)
National associations

Privacy and Security Policy

SECTION II – PHYSICAL SAFEGUARDS

SECURITY GUIDELINES

Facility

- Secure gated/enclosed area for loading and unloading the pickup/delivery vans.
- Non-hazardous industries near facility
- Site outside 100 year flood plain and not located in an area of river or lake flood potential
- Building sprinkler system according to local fire codes, with adequate water supply
- Exterior perimeter fencing and lighting for security protection
- Sprinkler and fire protection system
- Leak proof roof which provides water proof environment for storage of paper documents
- Intrusion protection includes central station alarm, perimeter entry contact alarms, interior motion detectors, closed circuit TV, key pad/access card door systems, manual fire pulls, window glass break detectors
- Quarterly sprinkler and alarms inspections
- Fire extinguishers in place – inspected quarterly
- No smoking policy posted/enforced
- Life safety signage – Personnel exit doors
- Shelving professionally installed and loaded based on weight restrictions
- Record center provides for emergency, holiday, after-hours access 365 days
- All required insurance coverage maintained

Privacy and Security Policy

SECTION II – PHYSICAL SAFEGUARDS

SECURITY GUIDELINES

Equipment

- Proper equipment provided for record center activities performed
- Material handling equipment inspected and maintained
- Safety and training provided to employees on all material handling equipment
- Lift truck/picker operators must complete approved safety training course
- Warehouse employee orientation includes safe lifting and carrying techniques, portable ladder safety and accident prevention tips
- Vehicle safety logs maintained
- All employees review general warehouse safety rules

Training

- Driver and warehouse employees trained on proper work flow and security of customer records/data
- All office and warehouse employees counseled quarterly on confidential nature of client records

Privacy and Security Policy

SECTION II – PHYSICAL SAFEGUARDS

SECURITY GUIDELINES

Facility Specifications

AARM Records Storage Center
15580 E. Hinsdale Circle
Centennial, CO 80112

Record Center

91,780 square feet leased multi-tenant facility
18,000 square feet office space
7 ½" concrete tilt walls with steel columns & joists
9 dock doors– 7 dock levelers
Clear height 22'9" – 24'6" / Column spacing 30' x 42'
Floors 6" thick 4000 psi concrete with welded wire mesh
ESFR Sprinkler system ((semi-annual inspections by ADT)
Fire extinguishers maintained by Western States Fire
Racked facility – mezzanine system
Monthly extermination – self administered
Roof – 22 gauge steel deck with R11 ISO-board & Perlite insulation and 4 ply glass fiber membrane

Media Vault

Stand-alone six sided block filled concrete vault
4 Hour Fire Rated
Climate and Humidity Controls
FM-200 CO2 Fire Protections System
CCTV Inside Vault and Card Key Access
Media Container Racks and Gemtrac Units
Restricted Access

Security System

ADT Master Security Control Panel
Outdoor siren / Indoor siren
Line cut monitor / Manual Fire Pull
Glass break detectors in office areas
Motion detectors – general office area
Overhead warehouse door contacts with magnets
Door day alarm – all warehouse entry doors
Central station monitoring – ADT

Privacy and Security Policy

SECTION II – PHYSICAL SAFEGUARDS

SECURITY GUIDELINES

Facility Specifications

Key scan Access Control

Key scan door controller
Card reader
Controlled access by shift
Duel master intercom for warehouse and office access doors
System wired to fire control panel

Closed Circuit TV

Phillips 1/3” Black and white camera
15 cameras with 2.8-8mm lenses (office/warehouse)
VAC power supply
ATV camera multiplexer
DVR – 30 day monitoring

Privacy and Security Policy

SECTION II – PHYSICAL SAFEGUARDS

SECURITY GUIDELINES

Fire Protection Security

Control valves. A sprinkler system must be capable of shut down after the fire has been controlled, and for periodic maintenance and modification. In the simplest system a single shutoff valve may be located at the point where the water supply enters the building. In larger buildings the sprinkler system may consist of multiple zones with a control valve for each. Control valves should be located in readily identified locations to assist responded emergency personnel.

These shut down controls should be locked in the open position. Keys for these locks should be placed in a readily available location for emergency access.

Tamper alarms should be installed on the control systems to notify the record center staff of an unauthorized system shut down.

Privacy and Security Policy

SECTION III – TECHNOLOGY SAFEGUARDS

RECORDS MANAGEMENT SOFTWARE SECURITY

Records Center Users

Records center software contains employee logon security while allowing all or restricted access to applications within software. Network administrator provides login/password assignments and will be responsible for the removal of login permissions upon employee termination.

Barcode technology is utilized to scan/track all actions performed – inbound, outbound and relocations within center. Historical tracking on all barcodes (containers/files) are maintained within database indicating login code, date, time and specific record data.

Client Users

Authorized Access Form is completed and signed by company officer indicating employees as “authorized requestors” for company records. Limitations can be placed on requests to the department level and even to specific container/file level. Authorized list is entered into records management software and once record request is made, window appears indicating “authorized users”.

Customer records retention policies and records series requirements can be maintained by system. Record expiration reports for containers/files are created, printed and sent to customer for removal/destruction authorization. Report should reflect “signature” field for each record. After destruction, automated Certificate of Destruction is available for printing. ***Only written authorizations for removal/destruction by authorized company officials will be accepted by records center.***

Client Web Users

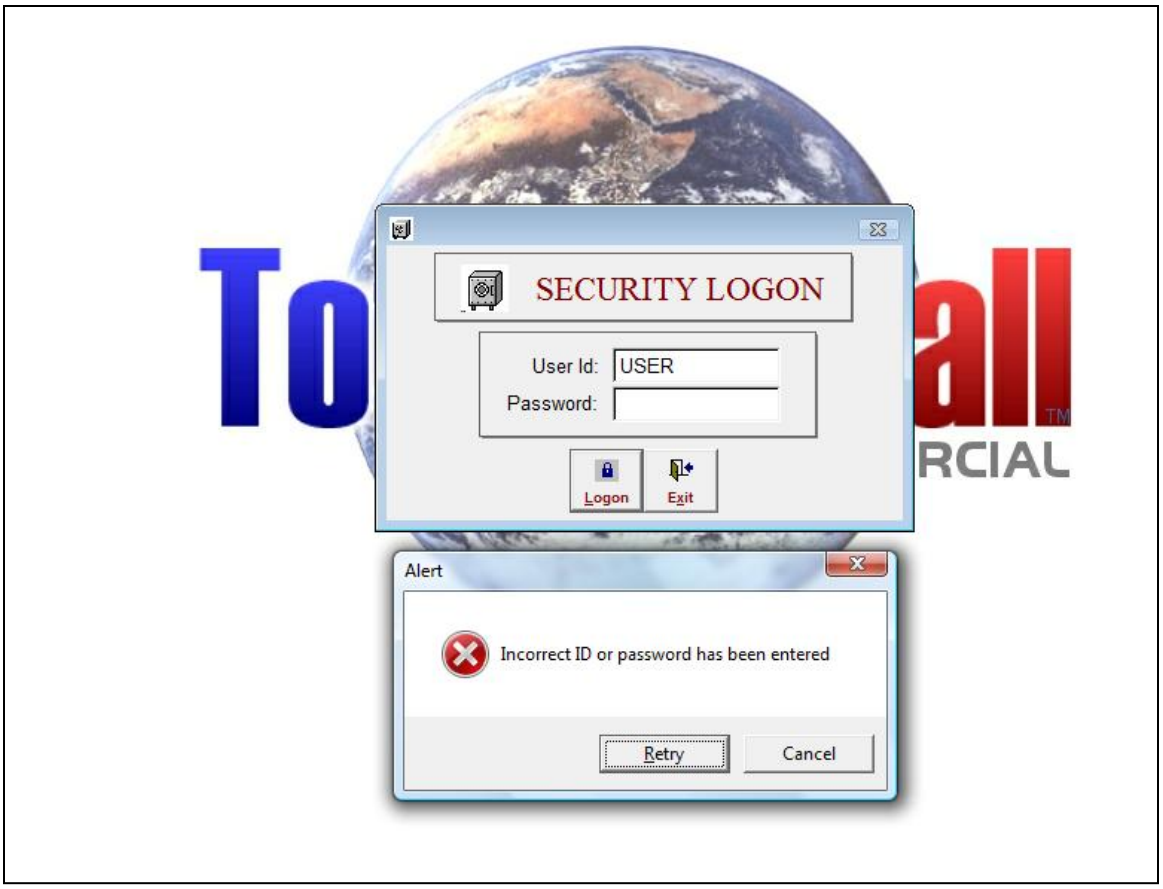
File/document images may also be viewed by customer over internet. In addition to performing data entry and placing Web requests, customers (pre-authorized administrative user) should be able to administer their own security logon/permissions, profiles and delivery site setup. Customers should be able to print or view on-line any image request with proper permissions and privileges previously setup. Reports can be created and printed by customer, based on user-defined parameters. Permissions to request or remove records through internet are set by client administrator only.

Privacy and Security Policy

SECTION III – TECHNOLOGY SAFEGUARDS

RECORDS MANAGEMENT SOFTWARE SECURITY

Valid user id and password must be provided by records center personnel to access records management software.



Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

ACCEPTABLE USE POLICY

Acceptable Use Policy

Overview

The intention of AARM for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to established culture of openness, trust and integrity. Our AARM is committed to protecting employees, partners, customers and AARM from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of AARM. These systems are to be used for business purposes in serving the interests of AARM, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at AARM. These rules are in place to protect the employee and AARM. Inappropriate use exposes AARM to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at AARM, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by AARM.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

ACCEPTABLE USE POLICY

Policy - General Use and Ownership

1. While AARM network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of AARM. Because of the need to protect AARM network, management cannot guarantee the confidentiality of information stored on any network device belonging to AARM.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. AARM recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within AARM may monitor equipment, systems and network traffic at any time, per AARM Audit Policy.
5. AARM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Policy - Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential, as defined by corporate confidentiality guidelines. Examples of confidential information include but are not limited to: AARM private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with AARM Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
6. Postings by employees from an AARM email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of AARM, unless posting is in the course of business duties.

7. All hosts used by the employee that are connected to the AARM Internet/Intranet/Extranet, whether owned by the employee or AARM, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Policy - Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of AARM authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing AARM owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

SYSTEM AND NETWORK ACTIVITIES

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or AARM protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by AARM.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AARM or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

ACCEPTABLE USE POLICY

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using an AARM computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any AARM account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to AARM is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, AARM employees to parties outside AARM.

EMAIL AND COMMUNICATION ACTIVITIES

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within AARM networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by AARM or connected via AARM network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

ACCEPTABLE USE POLICY

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

Revision History

Created 06/22/07

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

EMAIL RETENTION POLICY

Email Retention Policy

Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager.

Scope

This email retention policy is secondary to AARM policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All AARM email information is categorized into four main classifications with retention guidelines:

- Administrative Correspondence (4 years)
- Fiscal Correspondence (4 years)
- General Correspondence (1 year)
- Ephemeral Correspondence (Retain until read, destroy)

Policy

Administrative Correspondence
AARM Administrative Correspondence includes, though is not limited to clarification of established AARM policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox admin@AARM has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

Fiscal Correspondence
AARM Fiscal Correspondence is all information related to revenue and expense for the AARM. To ensure Fiscal Correspondence is retained, a mailbox fiscal@company has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

EMAIL RETENTION POLICY

General Correspondence
AARM General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

Ephemeral Correspondence
AARM Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

Instant Messenger Correspondence
<AARM Name> Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address.

Encrypted Communications
<AARM Name> encrypted communications should be stored in a manner consistent with <AARM Name> Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

Recovering Deleted Email via Backup Media
<AARM Name> maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Terms and Definitions

Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within AARM is done via a license. Please contact the appropriate support organization if you require a license.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

EMAIL RETENTION POLICY

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of AARM.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

DATABASE PASSWORD POLICY

Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of AARM networks.

Computer programs running on AARM networks often require the use of an internal database server. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

Scope

This policy applies to all software that will access an AARM, multi-user production database.

Policy - General

In order to maintain the security of AARM internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

Policy - Specifications

Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the Password Policy.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

DATABASE PASSWORD POLICY

Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

- For languages that execute from source code, the credentials' source file must not reside in the same browse able or executable file directory tree in which the executing body of code resides.

Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the Password Policy.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

DATABASE PASSWORD POLICY

Definitions

Term	Definition
Computer language	A language used to generate programs.
Credentials	Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.
Executing body	The series of computer instructions that the computer executes to run a program.
Hash location.	An algorithmically generated number that identifies a datum or its
LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories.
Module	A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Production	Software that is being used for a purpose other than when software is being implemented or tested.

Revision History

Created 06/22/07

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

ANTI-VIRUS GUIDELINES

Recommended processes to prevent virus problems:

- Always run the installed standard, supported anti-virus software. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in conjunction with AARM Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a CD or floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe offsite location.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

SERVER SECURITY POLICY

Server Security Policy

Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by AARM. Effective implementation of this policy will minimize unauthorized access to AARM proprietary information and technology.

Scope

This policy applies to server equipment owned and/or operated by AARM, and to servers registered under any AARM owned internal network domain.

Policy - Ownership and Responsibilities

All internal servers deployed at AARM must be owned by the operational group that is responsible for its system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by AARM. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by AARM.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

Policy - General Configuration Guidelines

- Operating System configuration should be in accordance with approved guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

SERVER SECURITY POLICY

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Policy - Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week.
  - Daily incremental tape backups will be retained for at least 1 month.
  - Weekly full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to AARM, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

Compliance

- Audits will be performed on a regular basis by authorized organizations within AARM.
- Audits will be managed by the internal audit group or AARM, in accordance with the Audit Policy. AARM will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

SERVER SECURITY POLICY

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	*Definition*
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal AARM Server. Desktop machines are not relevant to the scope of this policy.

Revision History

Create 06/22/07

Privacy and Security Policy

SECTION III – TECNOLOGY SAFEGUARDS

SECURITY RISK ASSESSMENT POLICY

Purpose

To empower AARM to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Scope

Risk assessments can be conducted on any entity within AARM or any outside entity that has signed a Third Party Agreement with AARM. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Policy

The execution, development and implementation of remediation programs are the joint responsibility of AARM and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the AARM Risk Assessment Team in the development of a remediation plan.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Terms	***Definitions***
Entity	Any business unit, department, group, or third party, internal or external to AARM, responsible for maintaining AARM assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of AARM key information assets and systems. AARM is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

Revision History

Created 06/22/07

All American Records Management

is Hereby Granted **NAID AAA Certification**®
by i-SIGMA®

The National Association for Information Destruction (NAID®) is the non-profit trade association recognized globally as the secure data destruction industry's standards setting and oversight body.

*The certificate holder has met the rigorous requirements of the NAID AAA Certification program and demonstrated through announced and unannounced audits that its security processes, procedures, systems, equipment, and training meet the standards of care required by all known data protection regulations.**

As a result, NAID AAA Certification also serves to meet all data controller vendor selection due diligence regulatory requirements.

The certificate holder is NAID AAA Certified for the following services and media types:

- Mobile Operation Endorsement for Paper/Printed Media Destruction
- Facility-based Operation Endorsement for Paper/Printed Media Destruction

Valid Through: 30 April 2023

Robert J. Johnson
NAID AAA Certification Program Official

Applicable to the following location(s):

- 15580 E Hinsdale Cir., Centennial, CO 80112 USA

*NAID AAA Certification specifications are regularly evaluated/amended as necessary and service provider compliance is verified to ensure ongoing conformance with all known data protection regulations including The Privacy Act (Australia), GDPR (Europe), HIPAA, GLBA, FACTA, State-level requirements (USA), and PIPEDA, PIPA, PHIPA (Canada) in their relevant jurisdiction(s), as well as with related risk assessment, incident reporting and data breach reporting procedures and training as required therein or separately.

EXHIBIT F - PRICING

All American
Records Management

ARCHIVE FEES				
BILLED MONTHLY IN ADVANCE				
SERVICE CODE		DESCRIPTION	PRICE	UNIT
SR		RENTENTION BASED ON PER CUBIC FOOT-	$0.0992	CUBIC FT/MONTH
DELIVERY FEES				
MAY INCLUDE FUEL SURCHARGE				
SERVICE CODE		DESCRIPTION	PRICE	UNIT
TRN		NEXT DAY DELIVERY OR PICKUP - INCLUDES 3 CUBIC FEET	$12.68	EVENT
TR1		NEXT DAY ITEMS OVER 3 CF	$0.88	CUBIC FT
TRS		SAME DAY DELIVERY OR PICKUP - INCLUDES 3 CUBIC FEET	$18.19	EVENT
TR2		SAME DAY ITEMS OVER 3 CF	$0.88	CUBIC FT
TRR		RUSH DELIVERY OR PICKUP - INCLUDES 3 CUBIC FEET	$44.10	EVENT
TR3		RUSH ITEMS OVER 3 CF	$0.88	CUBIC FT
TRA		AFTER HOURS DELIVERY OR PICKUP - INCLUDES 3 CUBIC FEET	$99.23	EVENT
TR4		AFTER HOURS ITEMS OVER 3 CF	$1.10	CUBIC FT
RECORD CENTER SERVICES FEES				
BILLED MONTHLY AS RENDERED				
SERVICE CODE		DESCRIPTION	PRICE	UNIT
RBN		BOX RETRIEVAL - NEXT DAY	$1.54	CUBIC FT
RBS		BOX RETRIEVAL - SAME DAY	$1.54	CUBIC FT
RBR		BOX RETRIEVAL - RUSH	$4.08	CUBIC FT
RBA		BOX RETRIEVAL - AFTER HOURS	$9.92	CUBIC FT
RTN		CONTAINER RETURN AND REFILE	$1.54	CUBIC FT
RFN		FILE RETRIEVAL - NEXT DAY	$1.54	EACH
RFS		FILE RETRIEVAL - SAME DAY	$1.54	EACH
RFR		FILE RETRIEVAL - RUSH	$4.08	EACH
RFA		FILE RETRIEVAL - AFTER HOURS	$9.92	EACH
RTF		FILE REFILE	$1.54	EACH
PRM		PERMANENT WITHDRAWAL OF BOX FROM AARM TO CLIENT	$0.00	CUBIC FT
PRM		PERMANENT WITHDRAWAL OF BOX ALREADY AT CLIENT THAT WILL NOT BE RETURNED TO AARM	$0.00	CUBIC FT
FNF		UNSUCCESSFUL RETRIEVAL/REFILE	$3.31	EACH
IFI		NEW FILE ADDITION TO BOX SURCHARGE	$1.54	EACH
IDI		INTERFILING/NEW DOCUMENT ADDITIONS TO A FILE	$1.54	EACH
CPY		COPY CHARGE - IF CLIENT WANTS COPIES OF DOCUMENTS MADE	$0.66	PAGE
SCN		SCAN ON DEMAND - SCAN AND SEND FILE VIA SECURE EMAIL	$0.17	PAGE
IBI		NEW ITEM ADDED TO INVENTORY	$1.10	CUBIC FT
RBX		REPACK DAMAGED BOXES	$5.25	EACH
WRP		SHRINK WRAP/LOAD PALLETS	$49.61	EACH
RECORD/INVENTORY DESTRUCTION SERVICES				
BILLED MONTHLY AS RENDERED				
SERVICE CODE		DESCRIPTION	PRICE	UNIT
DST		BOX DESTRUCTION - CONFIDENTIAL SHREDDING OF A BOX	$1.05	CUBIC FT
RBN		DESTRUCTION RETREIVAL - PULL A BOX FROM INVENTORY AND VALIDATE BOX FOR DESTRUCTION	$1.54	CUBIC FT
STANDARD ACCOUNT FEES				
BILLED MONTHLY AS RENDERED				
SERVICE CODE		DESCRIPTION	PRICE	UNIT
CNF		CONFERENCE ROOM USE FOR INVENTORY REVIEW	$0.00	DAY
DAX		ACCOUNT DEACTIVATION FEE	$0.00	ITEM
DOCK		DOCKING FEE	$0.00	ITEM
F4		FUMIGATION/ODOR CONTROL OF INVENTORY	By Quote	QUOTE
IK		WEB PORTAL INVENTORY MANAGEMENT SETUP	$0.00	NO CHARGE
WN		WEB PORTAL INVENTORY MANAGEMENT MONTHLY CHARGE	$0.00	NO CHARGE
MRL		LABOR CHARGE RECORD CENTER	$33.08	EACH
MRL		LABOR CHARGE RECORD CENTER-SUPERVISOR	$49.61	EACH
CRA		RESEARCH/AUDITS/SPECIAL REPORTS	$41.90	EACH
ITEMS FOR PURCHASE				
BILLED MONTHLY AS RENDERED				
SERVICE CODE		DESCRIPTION	PRICE	UNIT
BX1		STANDARD PURPOSE BUILT RECORD STORAGE BOX - LEGAL LETTER 1.2 CUBIC FT	$3.50	EACH
BX2		STANDARD PURPOSE BUILT RECORD STORAGE BOX - LETTER 2.4 CUBIC FT	$6.00	EACH
PA		STANDARD 40" X 48" PALLET PURCHASE	$14.18	EACH
OL		ORDER BULK RECORD BOX LABELS	$0.00	NO CHARGE

NEXT DAY *Request by 4:00 PM deliver by 5:00 PM Next Day*
SAME DAY *Request by 11:00 AM, Deliver by 5:00 PM*
RUSH *Deliver within 2 hours of receipt of request*
AFTER HOURS *Delivery Requests outside normal business hours (8:00 AM to 5:00 PM)*

All American
Records Management

Shredding Pricing Schedule A

DESCRIPTION	PRICE
Executive Console	$13.25
65-gallon bin	$15.75
95-gallon bin	$18.00
Destruction per box 1.2 cubic foot box	$3.15
Destruction per box 2.4 cubic foot box	$6.30
Destruction per box 3.6 cubic foot box	$9.45
Purge Bins (per bin)	$47.25
Hard Drive Destruction	$10.50
CD Destruction	$0.105
LTO/DLT tape destruction	$1.05
Trip Charge (offsite)	$36.75
Trip Charge (onsite)	$52.50
After Hours Trip Charge	$157.50

All American
Records Management

Storage	Unit	Price
Case Storage: Small tape container (8-10 cap)	Per case, per month	$4.960
Case Storage: Large tape container (18 cap)	Per case, per month	$11.03
Tape Storage: Individual slotted tapes	Per tape, per month	$0.1700

Services-Vault Handling	Unit	Price
Case Retrieval	Per case	$1.10
Case Refile	Per case	$1.10
Tape Retrieval	Per Tape	$0.3900
Tape Refile	Per tape	$0.3900
Rush Case Retrieval	Per case	$2.21
Rush Tape Retrieval	Per Drive	$0.770
Transportation		
Daily M-F	Per stop	$16.54
Weekly 1 day per week Scheduled	Per stop	$22.05
Monthly 1 day per month Scheduled	Per stop	$33.08
Unscheduled Same day	Per stop	$66.15
2 Hour Rush	Per stop	$82.69
After Hours, Weekends	Per stop	$165.38
Holiday	Per stop	$220.50
Tape Case Rental, (2 case minimum)		
Small tape container 7/10 tapes	Per case, per month	$5.51
Large tape container 18 Tapes	Per case, per month	$11.03
Destruction		
Computer media: Includes certificate of destruction	Per item	$1.10
Additional services		
Admin Fee		No Charge
Fuel Surcharge		**No Charge**
Container Locks		**No Charge**

Note slots are billed increments of 32 in a case
and 40 out of case for LTO's

15580 E. Hinsdale Circle, Centennial, CO 80112 • Phone 303-373-5101 • www.aarmrecords.com

EXHIBIT G, BUSINESS ASSOCIATE AGREEMENT
HIPAA/HITECH

1. GENERAL PROVISIONS AND RECITALS.

1.01 The parties agree that the terms used, but not otherwise defined below, shall have the same meaning given to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and their implementing regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") as they exist or may hereafter be amended.

1.02 The parties agree that a business associate relationship (as described in 45 CFR §160.103) under HIPAA, the HITECH Act, and the HIPAA regulations arises between the CONTRACTOR and the CITY to the extent that CONTRACTOR performs, or delegates to subcontractors to perform, functions or activities on behalf of CITY.

1.03 CITY wishes to disclose to CONTRACTOR certain information, some of which may constitute Protected Health Information ("PHI") as defined below, to be used or disclosed in the course of providing services and activities.

1.04 The parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they exist or may hereafter be amended.

1.05 The parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that impose more stringent requirements with respect to privacy of PHI.

1.06 The parties understand that the HIPAA Privacy and Security rules apply to the CONTRACTOR in the same manner as they apply to a covered entity. CONTRACTOR agrees to comply at all times with the terms of this Agreement and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they exist or may hereafter be amended, with respect to PHI.

2. DEFINITIONS.

2.01 "Administrative Safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of CONTRACTOR's workforce in relation to the protection of that information.

2.02 "Agreement" means the attached Agreement and its exhibits to which these additional terms are incorporated by reference.

2.03 "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

2.03.1 Breach excludes:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of CONTRACTOR or CITY, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

2. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI, or organized health care arrangement in which CITY participates, and the information received as a result of such disclosure is not further used or disclosed in a manner disallowed under the HIPAA Privacy Rule.

3. A disclosure of PHI where CONTRACTOR or CITY has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.03.2 Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless CONTRACTOR demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

2.04 "CONTRACTOR" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.05 "CITY" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.06 "Data Aggregation" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.07 "Designated Record Set" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.08 "Disclosure" shall have the meaning given to such term under the HIPAA regulations in 45 CFR §160.103.

2.09 "Health Care Operations" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.10 "Immediately" where used here shall mean within 24 hours of discovery.

2.11 "Individual" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §160.l03 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

2.12 "Parties" shall mean "CONTRACTOR" and "CITY", collectively.

2.13 "Physical Safeguards" are physical measures, policies, and procedures to protect CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

2.14 "The HIPAA Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

2.15 "Protected Health Information" or "PHI" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

2.16 "Required by Law" shall have the meaning given to such term under the HIPAA Privacy Rule at 45 CFR §164.103.

2.17 "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

2.18 "Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computer networks or servers maintained by CONTRACTOR.

2.19 "The HIPAA Security Rule" shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.

2.20 "Subcontractor" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

2.21 "Technical safeguards" means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.

2.22 "Unsecured PHI" or "PHI that is unsecured" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services ("HHS") in the guidance issued on the HHS Web site.

2.23 "Use" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

3. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE.

3.01 CONTRACTOR agrees not to use or further disclose PHI that CITY discloses to CONTRACTOR except as permitted or required by this Agreement or by law.

3.02 CONTRACTOR agrees to use appropriate safeguards, as provided for in this Agreement, to prevent use or disclosure of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY, except as provided for by this Contract.

3.03 CONTRACTOR agrees to comply with the HIPAA Security Rule, at Subpart C of 45 CFR Part 164, with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY.

3.04 CONTRACTOR agrees to mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of PHI by CONTRACTOR in violation of the requirements of this Agreement that becomes known to CONTRACTOR.

3.05 CONTRACTOR agrees to immediately report to CITY any Use or Disclosure of PHI not provided for by this Agreement that CONTRACTOR becomes aware of. CONTRACTOR must report Breaches of Unsecured PHI in accordance with 45 CFR §164.410.

3.06 CONTRACTOR agrees to ensure that any of its subcontractors that create, receive, maintain, or transmit, PHI on behalf of CONTRACTOR agree to comply with the applicable requirements of Section 164 Part C by entering into a contract or other arrangement.

3.07 To comply with the requirements of 45 CFR §164.524, CONTRACTOR agrees to provide access to CITY, or to an individual as directed by CITY, to PHI in a Designated Record Set within fifteen (15) calendar days of receipt of a written request by CITY.

3.08 CONTRACTOR agrees to make amendment(s) to PHI in a Designated Record Set that CITY directs or agrees to, pursuant to 45 CFR §164.526, at the request of CITY or an Individual, within thirty (30) calendar days of receipt of the request by CITY. CONTRACTOR agrees to notify CITY in writing no later than ten (10) calendar days after the amendment is completed.

3.09 CONTRACTOR agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by CONTRACTOR on behalf of CITY, available to CITY and the Secretary in a time and manner as determined by CITY, or as designated by the Secretary, for purposes of the Secretary determining CITY'S compliance with the HIPAA Privacy Rule.

3.10 CONTRACTOR agrees to document any Disclosures of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY, and to make information related to such Disclosures available as would be required for CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.

3.11 CONTRACTOR agrees to provide CITY information in a time and manner to be determined by CITY in order to permit CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.

3.12 CONTRACTOR agrees that, to the extent CONTRACTOR carries out CITY's obligation(s) under the HIPAA Privacy and/or Security rules, CONTRACTOR will comply with the requirements of 45 CFR Part 164 that apply to CITY in the performance of such obligation(s).

3.13 CONTRACTOR shall work with CITY upon notification by CONTRACTOR to CITY of a Breach to properly determine if any Breach exclusions exist as defined below.

4. SECURITY RULE.

4.01 CONTRACTOR shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR §164.308, §164.310, §164.312, §164.314 and §164.316 with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY. CONTRACTOR shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.

4.02 CONTRACTOR shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of CONTRACTOR agree through a contract with CONTRACTOR to the same restrictions and requirements contained here.

4.03 CONTRACTOR shall immediately report to CITY any Security Incident of which it becomes aware. CONTRACTOR shall report Breaches of Unsecured PHI as described in 5. BREACH DISCOVERY AND NOTIFICATION below and as required by 45 CFR §164.410.

5. BREACH DISCOVERY AND NOTIFICATION.

5.01 Following the discovery of a Breach of Unsecured PHI, CONTRACTOR shall notify CITY of such Breach, however, both parties may agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR §164.412.

5.01.1 A Breach shall be treated as discovered by CONTRACTOR as of the first day on which such Breach is known to CONTRACTOR or, by exercising reasonable diligence, would have been known to CONTRACTOR.

5.01.2 CONTRACTOR shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have been known, to any person who is an employee, officer, or other agent of CONTRACTOR, as determined by the federal common law of agency.

5.02 CONTRACTOR shall provide the notification of the Breach immediately to the CITY DEH Executive Director or other designee.

5.02.1 CONTRACTOR'S initial notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

5.03 CONTRACTOR'S notification shall include, to the extent possible:

5.03.l The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by CONTRACTOR to have been, accessed, acquired, used, or disclosed during the Breach;

5.03.2 Any other information that CITY is required to include in the notification to each Individual under 45 CFR §164.404 (c) at the time CONTRACTOR is required to notify CITY, or

promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR §164.410 (b) has elapsed, including:

1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

2. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

4. A brief description of what CONTRACTOR is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and

5. Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

5.04 CITY may require CONTRACTOR to provide notice to the Individual as required in 45 CFR §164.404, if at the sole discretion of the CITY, it is reasonable to do so under the circumstances.

5.05 In the event that CONTRACTOR is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, CONTRACTOR shall have the burden of demonstrating that CONTRACTOR made all required notifications to CITY, and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not constitute a Breach.

5.06 CONTRACTOR shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR §164.402 to demonstrate that a Breach did not occur.

5.07 CONTRACTOR shall provide to CITY all specific and pertinent information about the Breach, including the information listed above, if not yet provided, to permit CITY to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after CONTRACTOR's initial report of the Breach to CITY.

5.08 CONTRACTOR shall continue to provide all additional pertinent information about the Breach to CITY as it becomes available, in reporting increments of five (5) business days after the prior report to CITY. CONTRACTOR shall also respond in good faith to all reasonable requests for further information, or follow-up information, after report to CITY, when such request is made by CITY.

5.09 In addition to the provisions in the body of the Agreement, CONTRACTOR shall also bear all expense or other costs associated with the Breach and shall reimburse CITY for all expenses CITY incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs or expenses associated with addressing the Breach.

6. PERMITTED USES AND DISCLOSURES BY CONTRACTOR.

6.01 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR as necessary to perform functions, activities, or services for, or on behalf of, CITY as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by CITY.

6.02 CONTRACTOR may use PHI that CITY discloses to CONTRACTOR, if necessary, for the proper management and administration of the Agreement.

6.03 CONTRACTOR may disclose PHI that CITY discloses to CONTRACTOR to carry out the legal responsibilities of CONTRACTOR, if:

6.03.1 The Disclosure is required by law; or

6.03.2 CONTRACTOR obtains reasonable assurances from the person or entity to whom/which the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person or entity and the person or entity immediately notifies CONTRACTOR of any instance of which it is aware in which the confidentiality of the information has been breached.

6.04 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR to provide Data Aggregation services relating to the Health Care Operations of CONTRACTOR.

6.05 CONTRACTOR may use and disclose PHI that CITY discloses to CONTRACTOR consistent with the minimum necessary policies and procedures of CITY.

7. OBLIGATIONS OF CITY.

7.01 CITY shall notify CONTRACTOR of any limitation(s) in CITY'S notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect CONTRACTOR'S Use or Disclosure of PHI.

7.02 CITY shall notify CONTRACTOR of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect CONTRACTOR'S Use or Disclosure of PHI.

7.03 CITY shall notify CONTRACTOR of any restriction to the Use or Disclosure of PHI that CITY has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect CONTRACTOR'S use or disclosure of PHI.

7.04 CITY shall not request CONTRACTOR to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by CITY.

8. BUSINESS ASSOCIATE TERMINATION.

8.01 Upon CITY'S knowledge of a material breach or violation by CONTRACTOR of the requirements of this Contract, CITY shall:

8.01.1 Provide an opportunity for CONTRACTOR to cure the material breach or end the violation within thirty (30) business days; or

8.01.2 Immediately terminate the Agreement, if CONTRACTOR is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.

8.02 Upon termination of the Agreement, CONTRACTOR shall either destroy or return to CITY all PHI CONTRACTOR received from CITY and any and all PHI that CONTRACTOR created, maintained, or received on behalf of CITY in conformity with the HIPAA Privacy Rule.

8.02.1 This provision shall apply to all PHI that is in the possession of subcontractors or agents of CONTRACTOR.

8.02.2 CONTRACTOR shall retain no copies of the PHI.

8.02.3 In the event that CONTRACTOR determines that returning or destroying the PHI is not feasible, CONTRACTOR shall provide to CITY notification of the conditions that make return or destruction infeasible. Upon determination by CITY that return or destruction of PHI is infeasible, CONTRACTOR shall extend the protections of this Agreement to the PHI and limit further Uses and Disclosures of the PHI to those purposes that make the return or destruction infeasible, for as long as CONTRACTOR maintains the PHI.

8.03 The obligations of this Agreement shall survive the termination of the Agreement.

9. <u>SUBSTANCE ABUSE (42 C.F.R., Part 2).</u>

CONTRACTOR shall also comply with all provisions of 42 C.F.R., Part 2 relating to substance abuse treatment and records.

EXHIBIT H, FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative